

Wireless P-T-P Ethernet Extender User Manual

Extend Ethernet links between buildings wirelessly and with ease.

Provides affordable point-to-point wireless Ethernet extension up to 6.2 miles (10 km).



Trademarks Used in this Manual

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Google Chrome is a registered trademark of Google Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation.

Firefox is a registered trademark of Mozilla Foundation.

Netscape is a registered trademark of Netscape Communications Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

About This Manual

This user manual helps the professional installer install the Wireless P-T-P Ethernet Extender and describes how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems. You can download this manual from ftp://ftp.blackbox.com/anonymous/manuals/L/LWE100A_rev1_user.pdf

A printed quick install guide is included with your Wireless P-T-P Ethernet Extender.

We're here to help! If you have any questions about your application or our products, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box." You'll be live with one of our technical experts in less than 30 seconds.

**FEDERAL COMMUNICATIONS COMMISSION
and INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS**

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

CAUTION: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad (Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá de lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquear la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - A: El cable de poder o el contacto ha sido dañado; u
 - B: Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - C: El aparato ha sido expuesto a la lluvia; o
 - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - E: El aparato ha sido tirado o su cubierta ha sido dañada.

Table of Contents

1. Specifications.....	7
1.1 General.....	7
1.2 Radio.....	7
1.3 Software.....	7
2. Overview.....	8
2.1 Introduction.....	8
2.2 Features.....	8
2.3 What's Included.....	8
2.4 Hardware Description.....	8
2.5 Typical Application.....	10
3. Hardware Installation.....	11
3.1 Preparing for Installation.....	11
3.2 Professional Installation Required.....	11
3.3 Safety Precautions.....	11
3.4 Installation Precautions.....	11
3.5 Hardware Installation Steps.....	11
3.5.1 Connect.....	11
3.5.2 Pole Mounting.....	14
3.5.3 Using the External Antenna.....	16
3.5.4 Using the Grounding Wire.....	17
4. Basic Settings.....	19
4.1 Factory Default Settings.....	19
4.2 System Requirements.....	20
4.3 Logging in to the Web-based Interface.....	20
4.4 Basic System Settings.....	21
4.5 Time Settings.....	24
4.6 RADIUS Settings.....	24
4.7 Firewall Settings.....	25
4.8 Basic Wireless Settings.....	29
4.9 Site Survey.....	31
4.10 VAP Profile Settings.....	31
4.11 VLAN Tab.....	33
5. Advanced Settings.....	34
5.1 Advanced Wireless Settings.....	34
5.2 Wireless Security Settings.....	35
5.2.1 Data Encryption and Authentication Settings.....	35
5.2.2 Access Control.....	37
5.2.3 WDS Settings.....	38
6. Management.....	39
6.1 Remote Management.....	39
6.2 SNMP Management.....	39
6.3 Coovachilli Settings.....	41
6.4 Upgrade Firmware.....	42
6.5 Backup/Retrieve Settings.....	42
6.6 Restore Factory Default Settings.....	43
6.7 Reboot.....	44

Table of Contents

- 6.8 Password 44
- 6.9 Certificate Settings 45
- 7. Monitoring Tools 46
 - 7.1 System Log 46
 - 7.2 Site Survey 46
 - 7.3 Ping Watchdog..... 47
 - 7.4 Data Rate Test 48
 - 7.5 Antenna Alignment..... 48
 - 7.6 Speed Test..... 49
- 8. Status 50
 - 8.1 View Basic Information 50
 - 8.2 View Association List..... 50
 - 8.3 View Network Flow Statistics 51
 - 8.4 View ARP Table 52
 - 8.5 View Bridge Table..... 52
 - 8.6 View Active DHCP Client Table..... 52
 - 8.7 View Network Activities 53
- 9. Troubleshooting 54
 - 9.1 Frequently Asked Questions 54
 - 9.2 Contacting Black Box..... 55
 - 9.3 Shipping and Packaging 55
- Appendix A. ASCII 56
- Appendix B. SSH Settings..... 57

1. Specifications

1.1 General

Standards — IEEE 802.3u MDI/MDI-X 10/100 Fast Ethernet, IEEE 80.11b/g wireless LAN interface, IEEE 802.1n draft wireless LAN standard

Temperature Tolerance — Operating: -4 to +158° F (-20 to +70° C);
Storage: -22 to +176° F (-30 to +80° C)

Humidity Tolerance — Operating: 10–95%;
Storage: 10–95%

Power — Input current: 0.5 A maximum;
Output Voltage: 15 V;
Output Current: 0.8 A

Size — 2.4"H x 2.5"W x 8.9"D (6.1 x 6.4 x 22.8 cm)

Weight — < 1.1 lb. (< 0.5 kg)

1.2 Radio

Antenna — Default embedded 8-dBi directional antenna (Vertical-Pol), reserve N-type connector (plug), software switchable

Modulation — IEEE 802.11b (DSSS): CCK, DQPSK, DBPSK;
IEEE 802.11g/n (OFDM/DSSS): QAM-16, QPSK, BPSK

Operating Frequency — IEEE 802.11b/g ISM Band; 802.11g/n 20 MHz;
U.S., Canada: 2.412 GHz–2.462 GHz;
EU: 2.412 GHz–2.472 GHz;
IEEE 802.11gn 40 MHz Band;
U.S., Canada: 2.422 GHz–2.452 GHz;
EU: 2.422 GHz–2.462 GHz

Output Power* — IEEE 802.11b: 27.5 dBm @ 11 Mbps;
IEEE 802.11g: 27.5 dBm @ 6 Mbps;
IEEE 802.11gn: 27.5 dBm @ HT20, 27.5 dBm @ HT40

*Band edge exclusive (controllable for different country regulations)

Sensitivity — IEEE 802.11b: -88 dBm @ 11 Mbps;
IEEE 802.11g: -73 dBm @ 6 Mbps;
IEEE 802.11n: -70 dBm @ HT20, -67 dBm @ HT40

1.3 Software

Advance Settings — Radio on/off, WMM/Regatta mode, output power control, fragmentation length, beacon interval, RTS/CTS threshold, DTIM interval

Management — Telnet, FTP, SMP, password changes, firmware updates, configuration files

Operation Mode — CPE, AP

Security — WEP 64, 128-bit, WPA/WPA2, WPA-PSK/WPA2-PSK, 802.1x authentication

2. Overview

2.1 Introduction

Designed for outdoor environment applications, the Wireless P-T-P Ethernet Extender is a high-performance last-mile broadband solution that provides reliable wireless network coverage. As an IEEE 802.11b/g compliant wireless device, the Wireless P-T-P Ethernet Extender is able to provide stable and efficient wireless performance. The extender delivers a much faster data rate than normal wireless devices and higher bandwidth with longer range for outdoor applications.

The Wireless P-T-P Ethernet Extender supports four wireless communication connectivity device types (AP, Wireless Client, Bridge and AP Repeater), allowing for various application requirements.

High output power and reliable performance make the Wireless P-T-P Ethernet Extender an ideal wireless broadband solution for wireless Internet service providers and system integrators.

2.2 Features

- Complies with IEEE 802.11b/g and IEEE 802.11n standards.
- Supports passive PoE, supplied with 12V.
- Highly reliable watertight housing endures almost any harsh environment.
- Four operating modes include AP, Wireless Client, WDS, and AP Repeater.
- Supports 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA & WPA2, WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK.
- Includes a user-friendly Web and SNMP-based management interface.

2.3 What's Included

Your package should contain the following items. If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

LWE100A or LWE100AE

- Wireless P-T-P Ethernet Extender
- Pole-mounting ring
- Power cord and PoE injector
- A printed Quick Installation Guide.

NOTE: You can download this user manual in PDF format from ftp://ftp.blackbox.com/anonymous/manuals/L/LWE100A_rev1_user.pdf

LWE100A-KIT or LWE100AE-KIT

- (2) Wireless P-T-P Extenders, preconfigured for bridging operation
- (2) pole-mounting rings
- (2) power cords and PoE injectors
- A printed Quick Installation Guide.

NOTE: The LWE100A-KIT and LWE100AE-KIT will be ready to deploy in bridging operation. Just plug them in with line-of-sight, and your connection will be established.

2.4 Hardware Description

Figure 2-1 shows the LWE100A. Figure 2-2 illustrates the pole mounting ring and Figure 2-3 shows the power cord and PoE injector. Table 2-1 describes these components.



Figure 2-1. LWE100A Ethernet extender.



Figure 2-2. Pole-mounting ring.

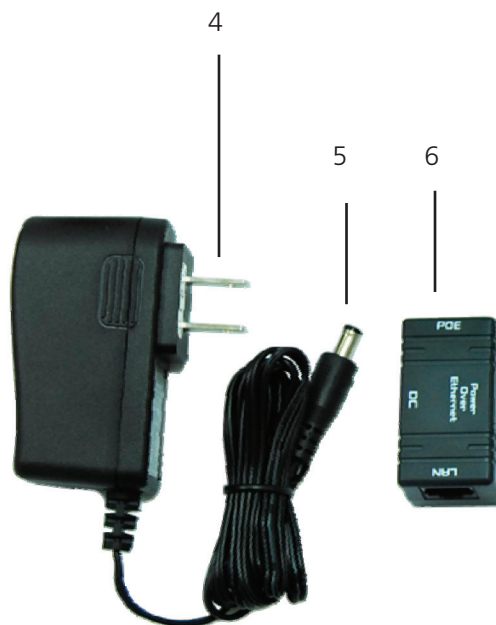


Figure 2-3. Power cord and PoE injector.

Table 2-1. Components.

Number	Component	Description
1	(1) reverse N-type connector	Ground the connector first, then install the antenna here.
2	(3) pole mounts	You will install the pole mounting ring through these mounts.
3	(1) pole mounting ring	Secures the extender to the pole
4	(1) U.S. power plug	Connects to a power source
5	(1) 2.5-mm barrel connector	Connects to the PoE injector
6	(1) Power over Ethernet (PoE) injector	Supplies power to the extender

WARNING: Users MUST use the power cord and PoE injector shipped in the box with the Wireless P-T-P Ethernet Extender. Using other options will damage the extender.

2.5 Typical Application

This section describes the typical applications of the Wireless P-T-P Ethernet Extender. By default, it is set to AP mode. This enables it to establish wireless coverage; plus, it is also able to join any available wireless network under wireless client mode. The Wireless P-T-P Ethernet Extender is able to deliver stable and efficient broadband connectivity for various applications.

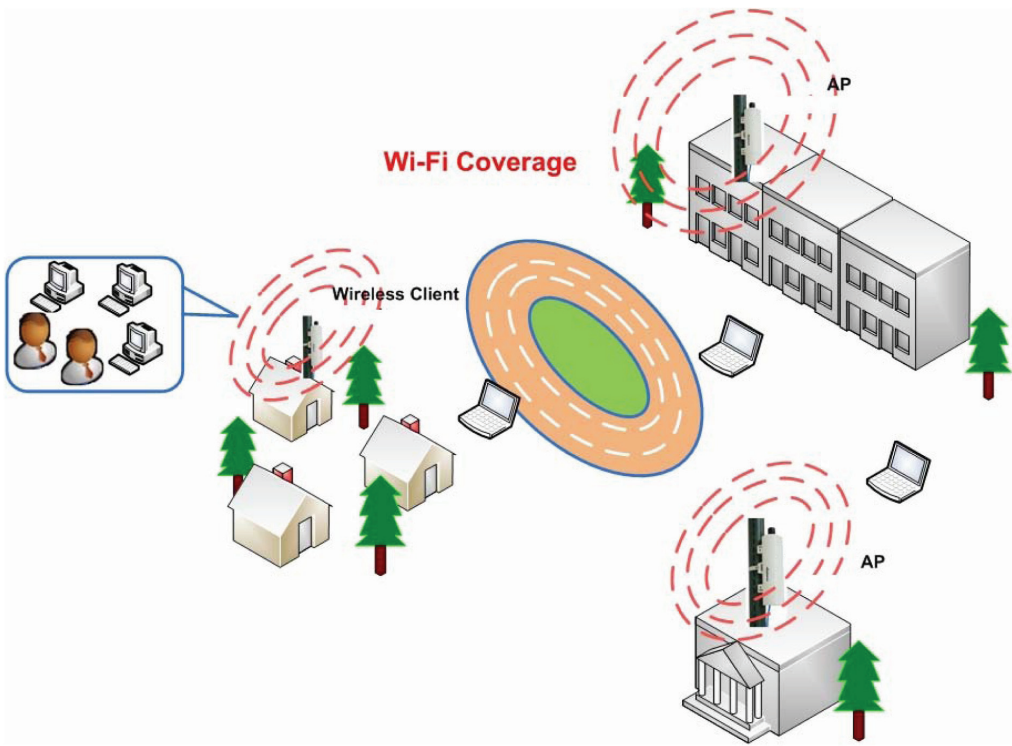


Figure 2-4. Wireless P-T-P Ethernet Extender application.

The Wireless P-T-P Ethernet Extender can also be used in the following environments:

- Cost-effectively provide long distance backhaul for remote areas (for example, a village, oil well, island, mountain, etc.).
- Establish local backhaul for campus, farm, and factory.
- Provides access for video streaming or surveillance for industrial and mining enterprises.

3. Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing the Wireless P-T-P Ethernet Extender.

3.1 Preparing for Installation

Read this chapter before installing the extender. It describes safety precautions and needed product information.

3.2 Professional Installation Required

Use a professional installer who is well trained in the RF installation and knowledgeable about local regulations.

3.3 Safety Precautions

To keep you safe and to install the hardware properly, read and follow these safety precautions.

1. If you are installing the Wireless P-T-P Ethernet Extender for the first time, for your safety as well as others', use a professional installer who is trained on the safety hazards involved.
2. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
3. When installing the Wireless P-T-P Ethernet Extender, note the following things:

NOTES:

Do not use a metal ladder;

Do not work on a wet or windy day;

Wear shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.

4. When the system is operating, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

3.4 Installation Precautions

Read and follow these installation precautions.

WARNING: EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

1. Users **MUST** use a proper and well-installed grounding and surge arrestor with the Wireless P-T-P Ethernet Extender, otherwise, a random lightning could easily cause fatal damage to Wireless P-T-P Ethernet Extender.
2. Users **MUST** use the power cord and PoE injector shipped in the box with the Wireless P-T-P Ethernet Extender. Using other components will cause damage to the extender.
3. Users **MUST** power off the Wireless P-T-P Ethernet Extender first before connecting the external antenna to it. Do not switch from the built-in antenna to the external antenna via Web management without physically attaching the external antenna onto the Wireless P-T-P Ethernet Extender, otherwise, the extender might be damaged.

3.5 Hardware Installation Steps

3.5.1 Connect

1. On the bottom of the Wireless P-T-P Ethernet Extender is a movable cover. Grab the cover and pull it back gently to remove it as shown in Figure 3-1.

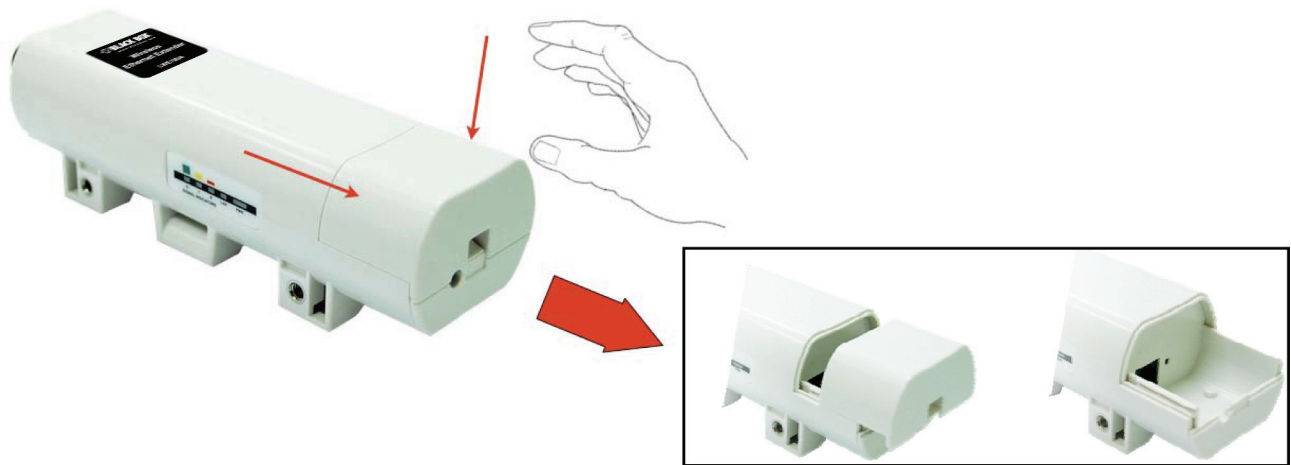


Figure 3-1. Removing the bottom cover.

2. Plug a standard Ethernet cable into the RJ-45 port. See Figure 3-2.



Figure 3-2. Plugging in the cable.

3. Slide the cover back to seal the bottom of the Wireless P-T-P Ethernet Extender.



Figure 3-3. Replacing the cover.

4. Take out the power cord and PoE injector, and plug the power cord into the DC port of the PoE injector as the right-side picture in Figure 3-4 shows.



Figure 3-4. Installing the power cord and PoE injector.

5. Put what you assembled in step 3 and step 4 together by plugging the other side of the Ethernet cable from step 3 into the PoE port of the PoE injector shown in step 4. When you finish step 5, the extender, power cord, and PoE injector will appear as shown in Figure 3-5.



Figure 3-5. Extender.

3.5.2 Pole Mounting

1. Turn the Wireless P-T-P Ethernet Extender over. Put the pole mounting ring through the middle hole of the Wireless P-T-P Ethernet Extender.

NOTE: Use a screwdriver to unlock the pole-mounting ring before putting it through the Wireless P-T-P Ethernet Extender as the right-side picture in Figure 3-6 shows.

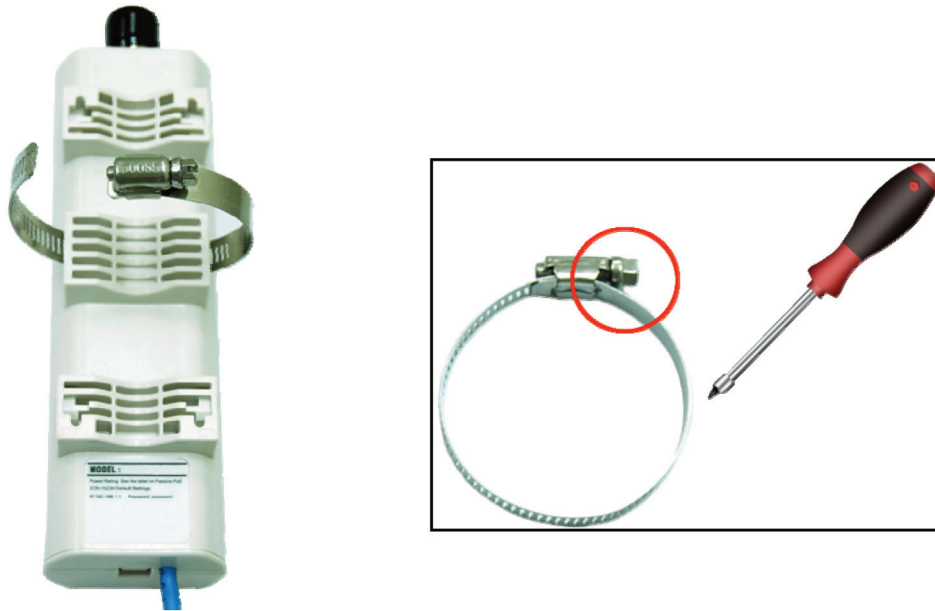


Figure 3-6. Unlocking the pole-mounting ring.

2. Mount the Wireless P-T-P Ethernet Extender firmly to the pole by locking the pole mounting ring tightly.

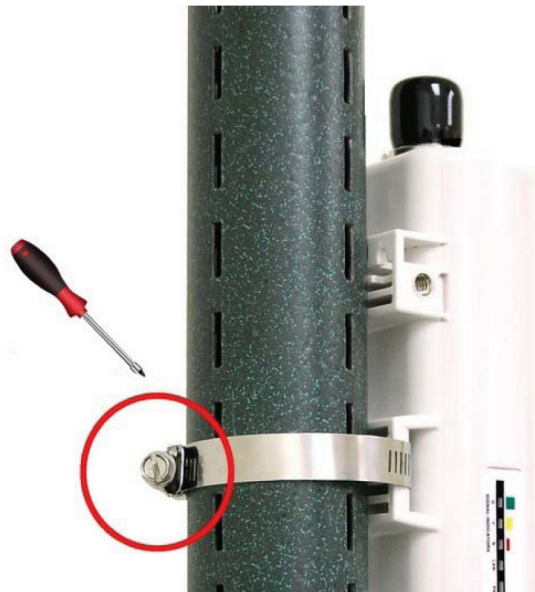


Figure 3-7. Mounting the extender to a pole.

3. When installation is complete, the extender should look like Figure 3-8.



Figure 3-8. Extender installed outdoors on a pole.

3.5.3 Using the External Antenna

If you prefer to use the external antenna with N-type connector for your application instead of the built-in directional antenna, follow the steps below.

1. Grab the black rubber on the top of the Wireless P-T-P Ethernet Extender, and slightly pull it up as shown in Figure 3-9. The metal N-type connector will appear.



Figure 3-9. Installing the external antenna.

2. Connect your antenna with the N-type connector on the top of the Wireless P-T-P Ethernet Extender.

NOTES:

1. Before connecting the external antenna with the N-type connector to the Wireless P-T-P Ethernet Extender, users should prepare the cable in advance, if needed.
2. While connecting the N-type connectors, users should be careful not to damage the connectors.

WARNING: Users **MUST** power off the Wireless P-T-P Ethernet Extender first before connecting the external antenna to it. Do not switch from the built-in antenna to the external antenna from Web management without physically attaching the external antenna onto the Wireless P-T-P Ethernet Extender. Otherwise, the Wireless P-T-P Ethernet Extender might be damaged.

3.5.4 Using the Grounding Wire

The Wireless P-T-P Ethernet Extender is shipped with a grounding wire. Properly ground the unit to protect against power surges.

1. Loosen and remove the metal O-ring on the N-type antenna connector.
2. Put the grounding wire into the connector and tighten it with the O-ring.



Figure 3-10. Connecting one end of the grounding wire.

3. Connect the other end of the grounding wire to the earth ground.



Figure 3-11. Connecting the other end of the grounding wire.

4. Basic Settings

4.1 Factory Default Settings

To return the extender to its factory-default settings, see Section 6.6.

Table 4-1. Wireless P-T-P Ethernet Extender Factory Default Settings.

Parameter	Default Setting
Username	admin
Password	password
Wireless Device Name	apXXXXXX (X represents the last 6 digits of the Ethernet MAC address)
Operating Mode	AP
Data Rate	Auto
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN Gateway	0.0.0.0
LAN Primary DNS Server	0.0.0.0
LAN Secondary DNS Server	0.0.0.0
Spanning Tree	Enable
802.11 Mode	802.11b/g/n
Channel Number	6
SSID	Wireless
Broadcast SSID	Enable
HT Protect	Disable
Data Rate	Auto
Output Power	Full
Channel Mode	20 MHz
WMM	Enabled
RTS Threshold (byte)	2346
Fragmentation Length (byte)	2346
Beacon Interval	100
DTIM Interval	1
Space in Meters	0
Flow Control by AP	Disable
Security	Open System
Encryption	None
Wireless Separation	Disable
Access Control	Disable
SNMP Enable/Disable	Enable
SNMP Read Community Name	Public
SNMP Write Community Name	Private
SNMP IP Address	0.0.0.0

Chapter 4: Basic Settings

4.2 System Requirements

Before configuration, make sure your system meets the following requirements:

- You will need a computer coupled with a 10/100 BASE-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x.

NOTE: The default IP address of Wireless P-T-P Ethernet Extender is 192.168.1.1. (X cannot be 0, 1, nor 255);

- A Web browser on a PC for configuration such as Microsoft® Internet Explorer® 6.0 or above, Netscape®, Firefox®, or Google Chrome®.

4.3 Logging Into the Web-based Interface

The Wireless P-T-P Ethernet Extender provides you with a user-friendly Web-based management tool.

Open a Web browser and enter the IP address (Default: 192.168.1.1) of the Wireless P-T-P Ethernet Extender into the address field. You will see the login page (Figure 4-1).



Wireless Broadband Access Point

Name

Password

Figure 4-1. Login page.

Enter the username (Default: admin) and password (Default: password) respectively and click “Login” to login to the main page of the Wireless P-T-P Ethernet Extender. This management interface provides five main options in the black bar, including Status, System, Wireless, Management, and Tools. See Figure 4-2.

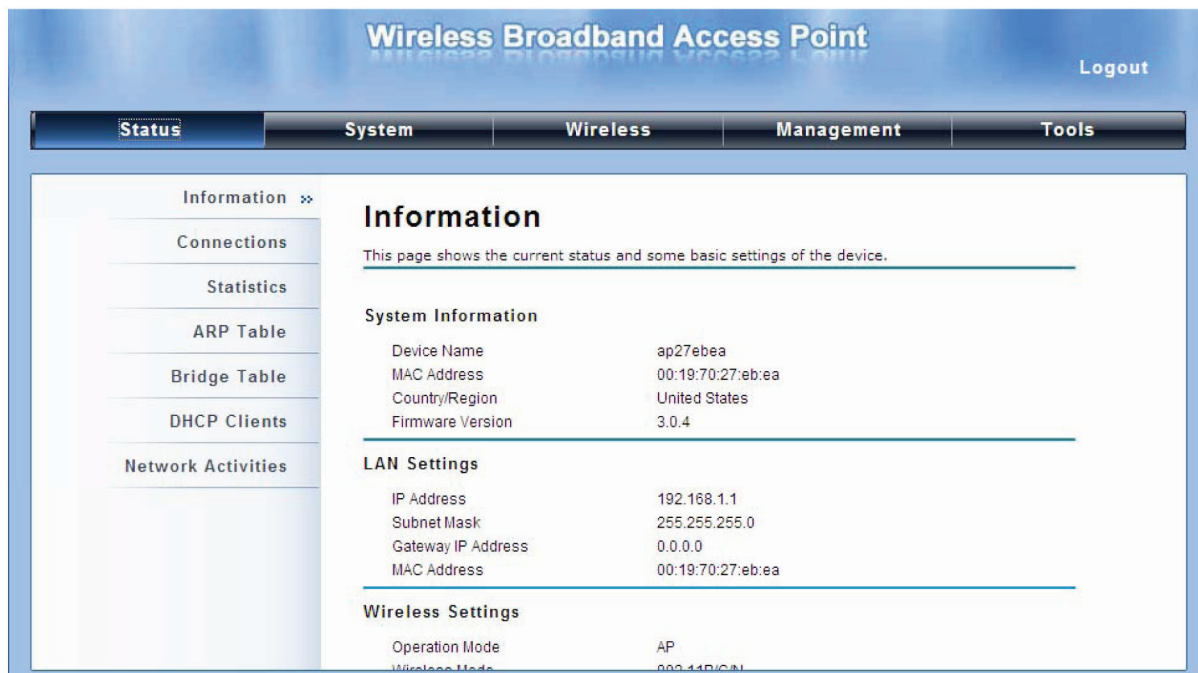


Figure 4-2. Main page.

NOTE: The username and password are case-sensitive, and the password should be no more than 19 characters.

4.4 Basic System Settings

If you are using the Wireless P-T-P Ethernet Extender for the first time, we recommend starting configuration from "Basic Settings" in the "System" screen shown next.

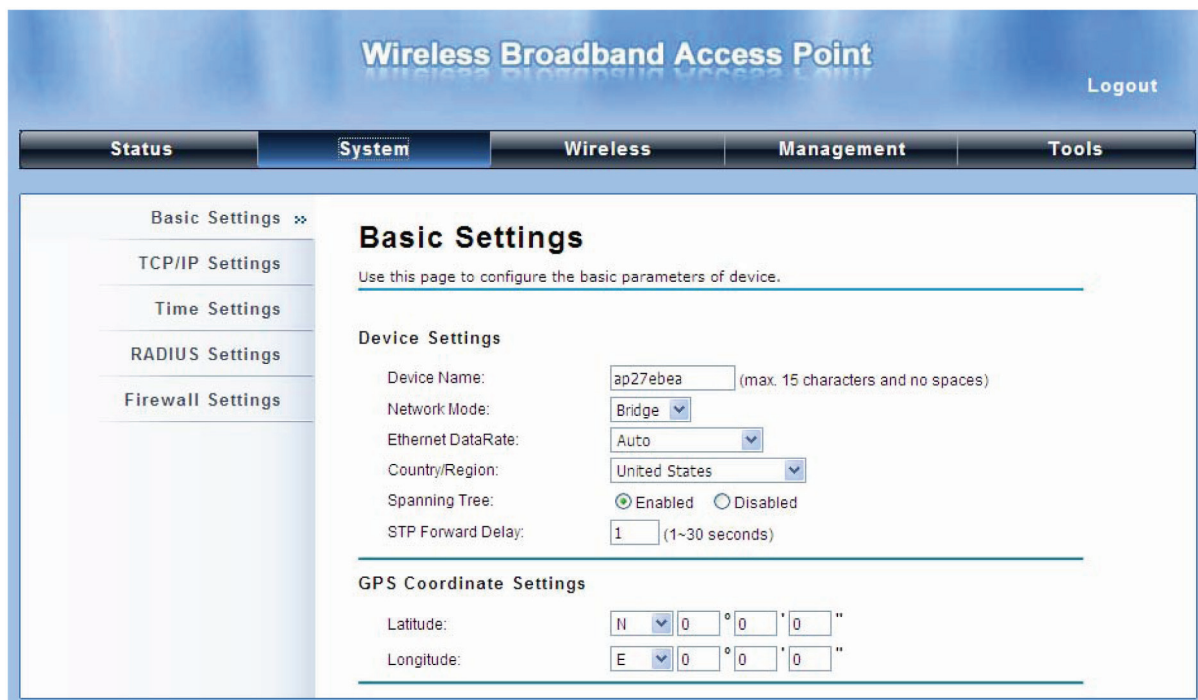


Figure 4-3. Basic system settings.

Chapter 4: Basic Settings

Basic Settings

- **Device Name:** Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z), or (-).
- **Network Mode:** Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to “TCP/IP Settings” below.
- **Ethernet Data Rate:** Specify the transmission rate of data for Ethernet. The default is “Auto.”
- **Country Region:** Available specific channels and/or operational frequency bands depend on the country where the extender is used.
- **Spanning Tree:** Spanning Tree Protocol (STP) is a link management protocol for AP that provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points, but establishes the redundant link as a backup if the initial link fails.
- **STP Forward Delay:** STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. The default time value is 1 sec.
- **GPS Coordinate Settings:** The GPS Coordinate Setting marks the latitude and longitude of the extender. Enter the coordinates and click the “Apply” button.

TCP/IP Settings

Open “TCP/IP Settings” in “System” as shown in Figure 4-4 to configure the parameters for the LAN that connects to the extender’s LAN port. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

The screenshot displays the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System' (selected), 'Wireless', 'Management', and 'Tools'. A 'Logout' link is in the top right. The left sidebar shows 'Basic Settings' (selected), 'TCP/IP Settings' (with a double arrow), 'Time Settings', 'RADIUS Settings', and 'Firewall Settings'. The main content area is titled 'TCP/IP Settings' and contains the following text: 'Use this page to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..'. Under the 'IP Address Assignment' section, there are two radio buttons: 'Obtain IP Address Automatically' (unselected) and 'Use Fixed IP Address' (selected). Below these are five input fields: 'IP Address:' (192.168.1.1), 'Subnet Mask:' (255.255.255.0), 'Gateway Ip Address:' (0.0.0.0), 'DNS 1:' (0.0.0.0), and 'DNS 2:' (0.0.0.0). At the bottom right of the form are 'Apply' and 'Cancel' buttons.

Figure 4-4. TCP/IP settings (Bridge).

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option. This enables the Wireless P-T-P Ethernet Extender to obtain IP settings automatically from that DHCP server.

NOTES:

1. When the IP address of the extender is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For immediate access to the bridge, flush the netbios cache on the client computer by running the “nbtstat -r” command before using the device name of the CPE to access its Web management page.
2. If the IEEE 802.11b/g/n Wireless Outdoor CPE is unable to obtain an IP address from a valid DHCP server, it will fall back to default static IP address.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway, and DNS server for the extender manually. Make sure the specified IP address is unique on your network to prevent IP conflict.

If the IEEE 802.11b/g/n Wireless Outdoor CPE is configured in Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

Logout

Wireless Broadband Access Point

Status System **Wireless** Firewall Management Tools

Basic Settings
TCP/IP Settings »
Time Settings
RADIUS Settings

TCP/IP Settings

Use this page to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

WAN Settings:

WAN Access Type: Static IP

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

LAN Settings:

IP Address: 192.168.0.99

Subnet Mask: 255.255.255.0

DHCP Server: Disabled

DHCP IP Address Range: 0.0.0.0 - 0.0.0.0

Lease Time: 0 (15-44640 Minutes)

Figure 4-5. TCP/IP settings (Router).

WAN Settings: Specify the Internet access method to Static IP, DHCP, or PPPOE. Users must enter WAN IP Address, Subnet Mask, and Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify the IP address and the subnet mask for the extender manually. Make sure the specified IP address is unique on your network to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway, and Lease Time (15-44640 minutes). DHCP relay agents forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. To enable the DHCP relay agent, check the “Enable DHCP Relay” checkbox and enter the IP address of the DHCP server.

WARNING:

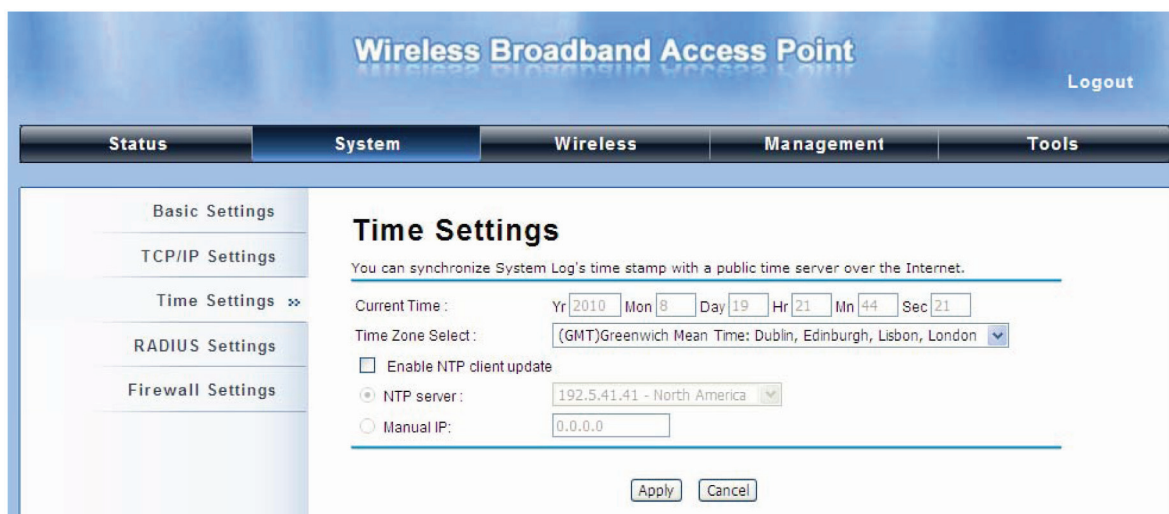
In AP mode, the Wireless P-T-P Ethernet Extender must establish a connection with another wireless device before it is set to Router mode. To access the unit in Router mode via a wired port, type the WAN IP address you will use to enter the Web page. The WAN is on a wired port and the LAN is on a wireless port. Or, you can access the device through the wireless device connected with the extender.

In wireless client mode, users can access the extender via its wired port. The WAN is on a wireless port and the LAN is on a wired port when the device is set to Router mode.

WARNING: Bridge mode and AP Repeater mode are similar to AP mode when the device is set to Router mode; the WAN is on wired port and the LAN is on wireless port. Users must also connect the extender with another wireless device before it is set to Router mode and access the extender via the connected wireless device.

4.5 Time Settings

Compliant with NTP, the Wireless P-T-P Ethernet Extender keeps time to match the Internet time. Configure the time in “Time Settings” from “System.” To use this feature, check “Enable NTP Client Update” in advance.



The screenshot shows the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The 'System' tab is selected, and the left sidebar shows 'Basic Settings', 'TCP/IP Settings', 'Time Settings' (with a double arrow), 'RADIUS Settings', and 'Firewall Settings'. The main content area is titled 'Time Settings' and contains the following fields:

- Current Time:** Yr 2010, Mon 8, Day 19, Hr 21, Mn 44, Sec 21
- Time Zone Select:** (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London (dropdown)
- ☐ Enable NTP client update
- ☒ NTP server: 192.5.41.41 - North America (dropdown)
- ☐ Manual IP: 0.0.0.0

At the bottom right of the form are 'Apply' and 'Cancel' buttons.

Figure 4-6. Time settings.

Current Time: Display the present time in Yr, Mon, Day, Hr, Min, and Sec.

Time Zone Select: Select the time zone from the dropdown list.

NTP Server: Select the time server from the “NTP Server” dropdown list or manually input the IP address of an available time server into “Manual IP.” Click on “Apply” to save the settings.

4.6 RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; it plays a central role in the network because it provides authenticating, authorizing, accounting, auditing, alarming, etc. It enables an organization to maintain user profiles in a central database that all remote servers can share.

Open “RADIUS Settings” in “System” to make RADIUS configuration.

The screenshot shows the 'Wireless Broadband Access Point' configuration interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings' (highlighted with a double arrow), and 'Firewall Settings'. The main content area is titled 'RADIUS Settings' and contains the following fields:

- Authentication RADIUS Server**
 - IP Address: 0.0.0.0
 - Port: 1812
 - Shared Secret: (empty field)
- ☐ **Global-Key Update**
 - every 3600 Seconds

At the bottom right of the form are 'Apply' and 'Cancel' buttons.

Figure 4-7. RADIUS settings.

Authenticating RADIUS Server

This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port, and Shared Secret.

IP Address: Enter the IP address of the Radius Server;

Port: Enter the port number of the Radius Server;

Shared Secret: This secret word or number (or a combination of letters and numbers), which is composed of no more than 31 characters, is shared by the Wireless P-T-P Ethernet Extender and RADIUS during authentication.

Global-Key Update: Check this option and specify the time interval between two global-key updates.

4.7 Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The Wireless P-T-P Ethernet Extender can provide Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding, as well as DMZ. This is available only under Router Mode.

Source IP Filtering: Source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through the Wireless P-T-P Ethernet Extender. Use these filters to help secure or restrict your local network.

The screenshot shows the 'Wireless Broadband Access Point' configuration interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering' (highlighted with a double arrow), 'Dst IP Filtering', 'Src Port Filtering', and 'Dst Port Filtering'. The main content area is titled 'Source IP Filtering' and contains the following text: 'Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' Below this text is a checkbox labeled 'Enable Source IP Filtering'. Underneath the checkbox are two input fields: 'Local IP Address:' and 'Comment:'. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table with four columns: 'Local IP Address', 'Comment', 'Select', and 'Edit'.

Figure 4-8. Source IP filtering.

Destination IP Filtering: Destination IP filtering gives you the ability to restrict the computers in a LAN from accessing certain Websites in a WAN according to specified IP addresses. Check the “Enable Source IP Filtering” checkbox and enter the IP address of the clients you want to restrict. Click on the “Apply” button to make the setting take effect.

The screenshot shows the 'Wireless Broadband Access Point' configuration interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering' (highlighted with a double arrow), and 'Src Port Filtering'. The main content area is titled 'Destination IP Filtering' and contains the following text: 'Entries in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address.' Below this text is a checkbox labeled 'Enable Destination IP Filtering'. Underneath the checkbox are two input fields: 'Destination IP Address:' and 'Comment:'. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table with four columns: 'Destination IP Address', 'Comment', 'Select', and 'Edit'.

Figure 4-9. Destination IP filtering.

Source Port Filtering: Source port filtering enables you to restrict certain ports of data packets from your local network to the Internet through the Wireless P-T-P Ethernet Extender. Use these filters to help secure or restrict your local network.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: Basic Settings, TCP/IP Settings, Time Settings, RADIUS Settings, Firewall Settings, Src IP Filtering, Dst IP Filtering, **Src Port Filtering** (highlighted with a double arrow), Dst Port Filtering, Port Forwarding, and DMZ Setting. The main content area is titled 'Source Port Filtering' and contains the following elements:

- A checkbox labeled 'Enable Source Port Filtering'.
- Input fields for 'Port Range' (two boxes separated by a hyphen) and 'Protocol' (a dropdown menu set to 'Both').
- A text input field for 'Comment'.
- 'Apply' and 'Cancel' buttons.
- A table with the following headers: 'Source Port Range', 'Protocol', 'Comment', 'Select', and 'Edit'.
- 'Delete Selected', 'Delete All', and 'Refresh' buttons at the bottom.

Figure 4-10. Source port filtering.

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to the Internet through the Wireless P-T-P Ethernet Extender. Use these filters to help secure or restrict your local network.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: Basic Settings, TCP/IP Settings, Time Settings, RADIUS Settings, Firewall Settings, Src IP Filtering, Dst IP Filtering, Src Port Filtering, **Dst Port Filtering** (highlighted with a double arrow), Port Forwarding, and DMZ Setting. The main content area is titled 'Destination Port Filtering' and contains the following elements:

- A checkbox labeled 'Enable Destination Port Filtering'.
- Input fields for 'Port Range' (two boxes separated by a hyphen) and 'Protocol' (a dropdown menu set to 'Both').
- A text input field for 'Comment'.
- 'Apply' and 'Cancel' buttons.
- A table with the following headers: 'Dest Port Range', 'Protocol', 'Comment', 'Select', and 'Edit'.
- 'Delete Selected', 'Delete All', and 'Refresh' buttons at the bottom.

Figure 4-11. Port forwarding.

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you want to host a Web server or mail server on the private local network behind Wireless P-T-P Ethernet Extender's NAT firewall.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', 'Dst IP Filtering', 'Src Port Filtering', 'Dst Port Filtering', 'Port Forwarding' (highlighted with a double arrow), and 'DMZ Setting'. The main content area is titled 'Port Forwarding' and contains a description: 'Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.' Below the description is a checkbox for 'Enable Port Forwarding'. There are input fields for 'IP Address', 'Protocol' (a dropdown menu set to 'Both'), 'Port Range' (two input boxes separated by a hyphen), and a 'Comment' field. At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a table with headers: 'Local IP Address', 'Protocol', 'Port Range', 'Comment', 'Select', and 'Edit'. At the very bottom are 'Delete Selected', 'Delete All', and 'Refresh' buttons.

Figure 4-12. Port forwarding.

DMZ: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists various settings: 'Basic Settings', 'TCP/IP Settings', 'Time Settings', 'RADIUS Settings', 'Firewall Settings', 'Src IP Filtering', and 'DMZ Setting' (highlighted). The main content area is titled 'DMZ' and contains a description: 'A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.' Below the description is a checkbox for 'Enable DMZ'. There is an input field for 'DMZ Host IP Address' with the value '0.0.0.0'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 4-13. DMZ.

4.8 Basic Wireless Settings

Open “Basic Settings” in “Wireless” to configure basic wireless.

The screenshot shows the 'Wireless Broadband Access Point' configuration web interface. The top navigation bar includes 'Status', 'System', 'Wireless' (selected), 'Management', and 'Tools'. A 'Logout' link is in the top right. On the left, a sidebar lists 'Basic Settings' (selected), 'Profile Settings', 'Advanced Settings', 'Access Control', and 'WDS Settings'. The main content area is titled 'Wireless Basic Settings' and contains a description: 'Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.' Below this is a checkbox for 'Disable Wireless LAN Interface'. The configuration options include: 'Wireless Mode' (AP), 'Wireless Network Name (SSID)' (Wireless), 'Broadcast SSID' (Enabled), '802.11 Mode' (802.11B/G/N), 'HT protect' (Disabled), 'Frequency/Channel' (2452MHz (9)), 'Extension Channel' (None), 'Channel Mode' (20 MHz), 'Antenna' (Internal (8 dBi)), and 'Maximum Output Power (per antenna)' (26 dBm).

Figure 4-14. Basic wireless settings.

Disable Wireless LAN Interface

Check this option to disable the WLAN interface. The wireless module of the Wireless P-T-P Ethernet Extender will then stop working and no wireless device can connect to it.

Wireless Mode

Four operating modes are available in the Wireless P-T-P Ethernet Extender.

AP: The Wireless P-T-P Ethernet Extender establishes a wireless coverage and receives connectivity from other wireless devices.

Wireless Client: The Wireless P-T-P Ethernet Extender can connect to the AP and join the wireless network around it.

Bridge: The Wireless P-T-P Ethernet Extender establishes wireless connectivity with other APs by keying in a remote MAC address. Refer to the “WDS Setting” in Section 5.2.3 for detailed configuration.

AP Repeater: The Wireless P-T-P Ethernet Extender servers as AP and Bridge concurrently. In other words, the extender can provide connectivity services for extenders in Bridge mode.

Wireless Network Name (SSID)

This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices.

NOTE: SSID is case-sensitive and cannot exceed 32 characters.

Broadcast SSID

In AP mode, you need to hide the network name when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the Wireless P-T-P Ethernet Extender, so that malicious attack by some illegal STA can be avoided.

Chapter 4: Basic Settings

802.11 Mode

The Wireless P-T-P Ethernet Extender can communicate with wireless devices that conform to 802.11b/g or 802.11b/g/n.

HT Protect

Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, the wireless client can be divided into HT STA and Non-HT STA. The one with HT protect enabled gets higher throughput.

Frequency/Channel

Channel varies because the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

Extension Channel

This channel only applies to AP, AP Repeater, and 40MHz channel width. Using channel bonding, it enables the Wireless P-T-P Ethernet Extender to use two channels at once. Two options are available: Upper Channel and Lower Channel.

Channel Mode

Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, so it might cause potential interference.

Antenna

By default, the Wireless P-T-P Ethernet Extender uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your application, you can switch from "Internal (8 dBi)" to "External (N-Type)."

When External (N-Type) is selected, an Antenna Gain bar will appear to allow you to specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations.

CAUTION: You are able to choose "External (N-Type)" only when you have installed the external antenna; otherwise, the Wireless P-T-P Ethernet Extender might be damaged.

NOTES:

The maximum output power will vary depending on the country selected to comply with the local regulation.

The output power here is counted from the RF single chain only, not including the 8-dBi internal antenna.

Maximum Output Power (per chain)

Specify the signal transmission power. The higher the output power is, the wider the area the signal can cover, but the power consumption will be greater accordingly.

Data Rate

Usually "Auto" is preferred. Under this rate, the Wireless P-T-P Ethernet Extender will automatically select the highest available rate to transmit. In some cases, however, when there is no great demand for speed, you can have a relatively low transmit rate to enable a longer distance.

Extension Channel Protection Mode

This is to avoid conflict with other wireless networks and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self, the transmission amount of CTS-RTS is much lower.

Enable MAC Clone

Available only under the wireless client mode, it hides the MAC address of the AP while displaying the one of an associated wireless client or the MAC address designated manually.

4.9 Site Survey

Under wireless client mode, the Wireless P-T-P Ethernet Extender is able to perform a site survey. It detects available information about the access points.

Open “Basic Settings” in “Wireless,” by clicking the “Site Survey” button beside the “Wireless Mode” option. The wireless site survey window will pop up with a list of available APs in the vicinity. Select the AP you want to connect to and click “Selected” to establish connection.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
<input type="radio"/>	aeap17	2412MHz(1)	00:24:01:df:67:8e	802.11B/G	-78	WPA
<input type="radio"/>	aeap18	2412MHz(1)	00:21:91:f6:f7:55	802.11B/G	-77	NONE
<input type="radio"/>	FRITZBox Fon WLAN 7270	2412MHz(1)	00:24:fe:46:b9:c8	802.11B/G/N	-75	WPA2
<input type="radio"/>	RT-G32	2437MHz(6)	20:cf:30:d6:5a:d0	802.11B/G	-62	WEP
<input type="radio"/>	MIS-AP2	2437MHz(6)	00:13:f7:8e:8d:d3	802.11B/G/N	-49	WPA2
<input type="radio"/>	HTC	2437MHz(6)	90:21:55:c2:3f:9c	802.11B/G	-81	NONE
<input type="radio"/>	DIR-635	2462MHz(11)	00:24:a5:b4:cf:77	802.11B/G	-64	WPA
<input type="radio"/>	Apple Network 873e69	2417MHz(2)	10:9a:dd:87:3e:69	802.11B/G/N	-75	WPA2
<input type="radio"/>	ASIX_WiFi	2422MHz(3)	00:1e:58:29:28:27	802.11B/G	-65	NONE

Figure 4-15. Site Survey.

4.10 VAP Profile Settings

Available in AP mode, the Wireless P-T-P Ethernet Extender allows up to 16 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, check the “Enable” box of the profile and click on the profile (for example, Profile 2) to configure wireless and security settings. Click on the “Apply” button to activate the profile.

The screenshot shows the 'VAP Profile Settings' page. The left sidebar contains a menu with 'Basic Settings', 'Profile Settings' (selected), 'Advanced Settings', 'Access Control', and 'WDS Settings'. The main content area has a title 'VAP Profile Settings' and a subtitle 'define each WLAN's attribute.'. Below this is a table with 10 rows, each representing a VAP profile. The columns are: #, Profile Name, SSID, Security, Vlan ID, and Enable. Profile 1 is selected and has its 'Enable' checkbox checked.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	Profile1	Wireless	Open System	0	<input checked="" type="checkbox"/>
2	Profile2	Wireless	Open System	0	<input type="checkbox"/>
3	Profile3	Wireless	Open System	0	<input type="checkbox"/>
4	Profile4	Wireless	Open System	0	<input type="checkbox"/>
5	Profile5	Wireless	Open System	0	<input type="checkbox"/>
6	Profile6	Wireless	Open System	0	<input type="checkbox"/>
7	Profile7	Wireless	Open System	0	<input type="checkbox"/>
8	Profile8	Wireless	Open System	0	<input type="checkbox"/>
9	Profile9	Wireless	Open System	0	<input type="checkbox"/>
10	Profile10	Wireless	Open System	0	<input type="checkbox"/>

Figure 4-16. VAP Profile settings.

The screenshot shows the 'VAP Profile1 Settings' page. The left sidebar contains a menu with 'Basic Settings', 'Profile Settings' (selected), 'Advanced Settings', 'Access Control', and 'WDS Settings'. The main content area has a title 'VAP Profile1 Settings' and a subtitle 'Basic Settings'. Below this are two sections: 'Basic Settings' and 'Security Settings'. The 'Basic Settings' section contains fields for Profile Name, Wireless Network Name (SSID), Broadcast SSID, Wireless Separation, WMM Support, and Max. Station Num. The 'Security Settings' section contains fields for Network Authentication, Data Encryption, and Key Type.

Basic Settings

Profile Name: Profile1

Wireless Network Name (SSID): Wireless

Broadcast SSID: ☒ Enabled ☐ Disabled

Wireless Separation: ☐ Enabled ☒ Disabled

WMM Support: ☒ Enabled ☐ Disabled

☐ Max. Station Num: 32 (0-32)

Security Settings

Network Authentication: Open System

Data Encryption: None

Key Type: Hex

Figure 4-17. VAP Profile1 settings.

Basic Settings

Profile Name: Name of the VAP profile.

Wireless Network Name: Enter the virtual SSID for the VAP.

Broadcast SSID: In AP mode, you need to hide the network name when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the Wireless P-T-P Ethernet Extender, so malicious attack by an illegal STA can be avoided.

Wireless Separation: Wireless separation enhances the security of network transmission. Under the mode (except wireless client mode), enable “Wireless Separation” to prevent the communication among associated wireless clients.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, so time-sensitive data, such as video/audio data, may own a higher priority than common data. To enable WMM, the wireless client should also support it.

Max. Station Number: By checking the “Max. Station Num,” the extender will only allow up to 32 wireless clients to associate with it for better bandwidth for each client. By disabling the checkbox, the extender will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

Security Setting

To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11a/n Wireless Outdoor CPE provides you with rock solid security settings. For detailed information, go to Section 5.2, Wireless Security Settings.

4.11 VLAN Tab

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN. To allow users on the VLAN to access the Web page of the Wireless P-T-P Ethernet Extender, you need to enable “Enable 802.1Q VLAN” and assign a management VLAN ID for your device. Make sure the assigned management VLAN ID is identical to your network VLAN ID to enable you to access the Web page of the Wireless P-T-P Ethernet Extender.

The screenshot shows the 'Wireless Broadband Access Point' configuration page. The 'Wireless' tab is selected. On the left, there is a sidebar with 'Basic Settings', 'Profile Settings' (selected), 'Advanced Settings', 'Access Control', and 'WDS Settings'. The main area displays a table of wireless profiles:

Profile	Mode	Open System	
8	Profile8	Wireless	Open System
9	Profile9	Wireless	Open System
10	Profile10	Wireless	Open System
11	Profile11	Wireless	Open System
12	Profile12	Wireless	Open System
13	Profile13	Wireless	Open System
14	Profile14	Wireless	Open System
15	Profile15	Wireless	Open System
16	Profile16	Wireless	Open System

Below the table, there is a checkbox labeled 'Enable 802.1Q VLAN' which is checked. Underneath it is a text field labeled 'Management VLAN ID:' with the value '2001'. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-18. Management VLAN ID.

5. Advanced Settings

5.1 Advanced Wireless Settings

Open “Advanced Settings” in “Wireless” to make advanced wireless settings.

The screenshot shows the configuration interface for a Wireless Broadband Access Point. The top navigation bar includes 'Status', 'System', 'Wireless' (selected), 'Management', and 'Tools'. A 'Logout' link is in the top right. The left sidebar contains 'Basic Settings', 'Profile Settings', 'Advanced Settings' (selected), 'Access Control', and 'WDS Settings'. The main content area is titled 'Wireless Advanced Settings' and includes a warning: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will take.' Below this, various settings are listed with radio buttons for 'Enabled' or 'Disabled' and input fields for numerical values.

Setting	Value	Range
A-MPDU aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
A-MSDU aggregation:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Short GI:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
RTS Threshold:	2346	(1-2347)
Fragment Threshold:	2346	(256-2346)
Beacon Interval:	100	(20-1024 ms)
DTIM Interval:	1	(1-255)
IGMP Snooping:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
RIFS:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Link Integration:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
TDM Coordination:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	

Figure 5-1. Advanced wireless settings.

A-MPDU/A-MSDU Aggregation

The data rate of your AP (except wireless client mode) could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, we do not recommend that you enable it.

Short GI

Under 802.11n mode, enable it to obtain a better data rate if there is no negative compatibility issue.

RTS Threshold

The Wireless P-T-P Ethernet Extender sends RTS (Request to Send) frames to certain receiving stations and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in bytes. Setting it too low may result in poor network performance. We recommend that you leave it at its default of 2346.

Fragmentation Length

Specify the maximum size in bytes for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. We recommend that you leave it at its default of 2346.

Beacon Interval

Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

DTIM Interval

Delivery Traffic Indication Message (DTIM) is contained in the data packets. It enhances the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

Preamble Type

It defines some details on the 802.11 physical layer. "Long" and "Auto" are available.

IGMP Snooping

Available in AP/Router mode, IGMP snooping is the process of listening to IGMP network traffic. When IGMP snooping is enabled, the AP will listen to IGMP membership reports, queries, and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

RIFS

RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

Link Integration

Available under AP/Bridge/AP repeater mode. Check "Enable" to monitor the Ethernet port connection. It can inform the associating wireless clients as soon as it disconnects.

TDM Coordination

Time-Division Multiplexing Technique (TDM) helps avoid packet collisions and sends the packets much more efficiently while enabling higher effective throughput rates. This function is only available in AP/CPE mode. We recommend that you enable TDM coordination when multiple extenders will connect to the AP in your application.

LAN2LAN CPE

LAN2LAN CPE mode enables packet forwarding at the Layer 2 level. It is transparent for all the Layer 2 protocols.

Space in Meters

To decrease the chances of data retransmission at long distances, the Wireless P-T-P Ethernet Extender can automatically adjust the proper ACK timeout value by specifying the distance between the two nodes.

Flow Control

This enables the administrator to specify the incoming and outgoing traffic limit by checking "Enable Traffic Shaping." This is only available in Router mode.

NOTE: We strongly recommend that you leave most advanced settings at their defaults except "Distance in Meters." Adjust the parameter for real distance; any modification may negatively impact the performance of your wireless network.

5.2 Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connection, the Wireless P-T-P Ethernet Extender has rock-solid security settings.

5.2.1 Data Encryption and Authentication Settings

Open "Profile Setting" in "Wireless" and enter "VAP Profile 1 Settings."

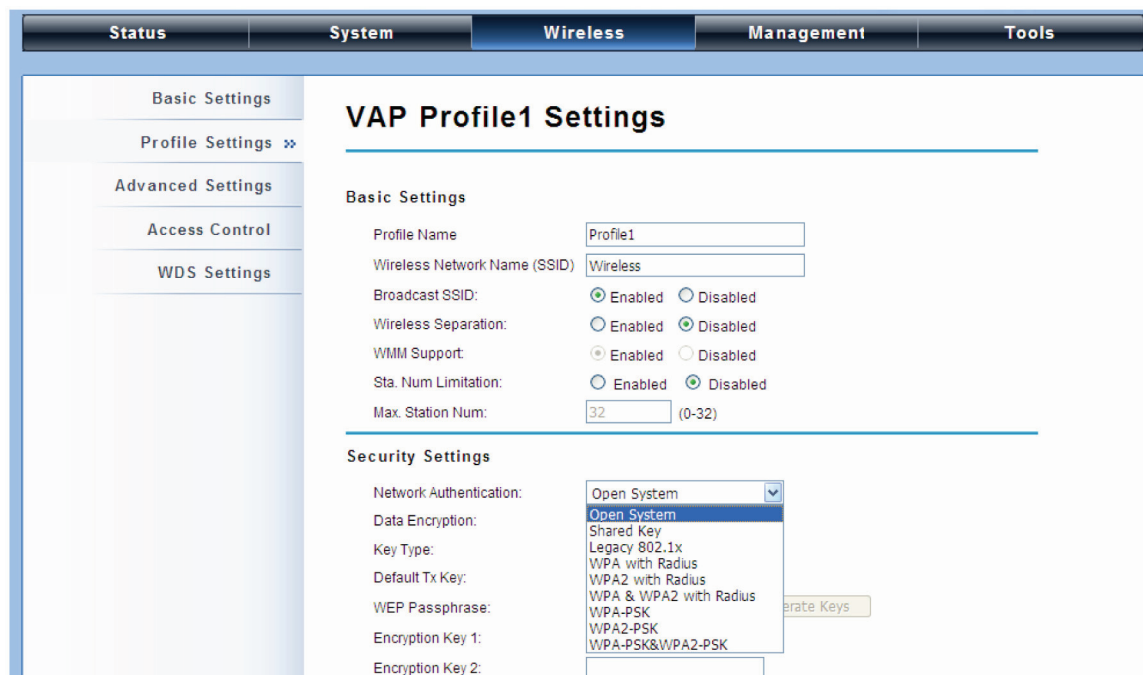


Figure 5-2. Security settings.

Network Authentication

Open System: This enables any device to join the network without performing a security check.

Shared Key: Data encryption and key are required for wireless authentication (not available in Bridge/AP Repeater mode).

Legacy 802.1x: Available in AP/Wireless Client mode, this provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication, and dynamic key management, it reduces the security risk of wireless networks to as low as possible. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP, and wireless client.

NOTE: For first time users, if EAP type "TLS" is selected, you need to import a valid user certificate. To import user certificates, refer to Section 6.9, Certificate Settings for more details.

WPA with RADIUS: Available in AP/Wireless Client mode, with warrant (username, password, etc.) offered by user, you can use this authentication with a specific RADIUS server.

This is commonly used in large enterprise networks.

WPA2 with RADIUS: Available in AP/Wireless Client mode, as a new version of WPA. If all the clients support WPA2, it is available. If it is selected, AES encryption and RADIUS server are required. It is only available in AP/Wireless Client mode.

WPA&WPA2 with RADIUS: Available in AP mode, it enables WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

WPA-PSK: This is a simplified WPA mode with no need for a specific authentication server. For the WPA Pre-Shared Key, pre-enter a key in each WLAN node. This is the commonly used in large and middle enterprise as well as a residential networks.

WPA2-PSK: As a new version of WPA, only available if all the clients support WPA2. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: Available in AP mode, it enables WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

Data Encryption

If data encryption is enabled, the key is required and only other devices using the the same key can communicate with each other.

None: Available only when the authentication type is open system.

64 bits WEP: Consists of 10 hexadecimal numbers.

128 bits WEP: Consists of 26 hexadecimal numbers.

152 bits WEP: Consists of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

AES: Advanced Encryption Standard; it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.

NOTES:

We strongly recommend that you enable wireless security on your network.

You can establish communicaton only by setting the same Authentication, Data Encryption, and Key in the Wireless P-T-P Ethernet Extender and other associated wireless devices.

5.2.2 Access Control

Access Control enables the wireless client to access the Wireless P-T-P Ethernet Extender, so a further security mechanism is provided. This function is available only under AP mode.

Open “Access Control” in “Wireless” as below.



Figure 5-3. Access Control.

Access Control Mode

If you select “Allow Listed,” only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “Deny Listed” is selected, those wireless clients on the list will not be able to connect the AP.

MAC Address

Enter the MAC address of the wireless client that you want to list into the access control list, click “Apply,” and it will be added into the table at the bottom.

Delete Selected/All

Check the box before one or more MAC addresses of wireless client(s) that you want to cancel, and click “Delete Selected” or “Delete All” to cancel that access control rule.

5.2.3 WDS Settings

Extend the range of your network without using cables to link the Access Points by using the Wireless Distribution System (WDS). Simply put, you can link the Access Points wirelessly. Open “WDS Settings” in “Wireless.”

The screenshot shows the 'Wireless Broadband Access Point' configuration interface. At the top, there's a header with the title and a 'Logout' link. Below the header is a navigation bar with tabs: 'Status', 'System', 'Wireless' (selected), 'Management', and 'Tools'. On the left side, there's a sidebar menu with options: 'Basic Settings', 'Profile Settings', 'Advanced Settings', 'Access Control', and 'WDS Settings' (which is expanded, showing a double arrow). The main content area is titled 'WDS Settings'. It contains a descriptive paragraph about WDS: 'Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS. This function can work only in Bridge and AP Repeater mode.' Below this text is a table with five rows for MAC addresses: 'Local MAC Address:', 'Remote AP MAC Address1:', 'Remote AP MAC Address2:', 'Remote AP MAC Address3:', and 'Remote AP MAC Address4:'. The first two fields are pre-filled with '00:19:70:00:fc:58' and '00:19:70:00:00:01' respectively. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 5-4. WDS Settings.

Enter the MAC address of another AP you want to connect wirelessly to into the appropriate field and click on the “Apply” button to save the settings.

NOTE: WDS Settings is available only under Bridge and AP Repeater Mode.

Bridge uses the WDS protocol that is not defined as the standard, so compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (that is, if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Avoid using mesh and ring network topologies, because they are not supported by WDS.

6. Management

6.1 Remote Management

The Wireless P-T-P Ethernet Extender provides remote management, including Telnet, SNMP, FTP, SSH, HTTPS, and exclusive WISE tool, making configuration more convenient and secure.

With "Normal" selected, Telnet, SNMP, and FTP are activated as default remote management options. To use secure management tools such as SSH, HTTPS and WISE, select "Secure." You can also choose "Customized" to enable any methods as desired.

Figure 6-1. Remote settings.

6.2 SNMP Management

The Wireless P-T-P Ethernet Extender supports SNMP for convenient remote management. Open "Remote Settings" in "Management" as shown below. Set the SNMP parameters and obtain the MIB file before remote management.

Figure 6-2. SNMP configuration.

Protocol Version

Select the SNMP version, and keep it identical on the Wireless P-T-P Ethernet Extender and the SNMP manager. The Wireless P-T-P Ethernet Extender supports SNMP v2/v3.

Server Port

Change the server port for a service if needed; however, you must use the same port to use that service for remote management.

Get Community

Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to “public” and allows all requests.

Set Community

Specify the password for the incoming Set requests from the management station. By default, it is set to “private.”

Trap Destination

Specify the IP address of the station to send the SNMP traps to.

Trap Community

Specify the password sent with each trap to the manager. By default, it is set to “public” and allows all requests.

Configure SNMPv3 User Profile

For SNMP protocol version 3, click “Configure SNMPv3 User Profile” to set the details for SNMPv3 user. Check “Enable SNMPv3 Admin/User” in advance, and continue configuring the extender.

The screenshot displays the configuration interface of a Wireless P-T-P Ethernet Extender, specifically the 'Management' tab. The left sidebar contains navigation links: 'Remote Settings >>', 'Firmware Upload', 'Configuration File', and 'Password Settings'. The main content area is titled 'Configure SNMPv3 User Profile'. It features two sections for user configuration. The first section, 'Enable SNMPv3Admin', is checked and includes fields for 'User Name' (SNMPv3Admin), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Access Type' (Read/Write), 'Authentication Protocol' (MD5), and 'Privacy Protocol' (None). The second section, 'Enable SNMPv3User', is also checked and includes fields for 'User Name' (SNMPv3User), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Access Type' (Read Only), 'Authentication Protocol' (MD5), and 'Privacy Protocol' (None). Above these sections, there are fields for 'Trap Destination' (0.0.0.0) and 'Trap Community' (public).

Figure 6-3. Configure SNMPv3 user profile.

User Name

Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the Wireless P-T-P Ethernet Extender.

Password: Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the Wireless P-T-P Ethernet Extender.

Confirm Password: Input that password again to make sure it is your desired one.

Access Type: Select "Read Only" or "Read and Write."

Authentication Protocol: Select an authentication algorithm. SHA authentication is stronger than MD5, but is slower.

Privacy Protocol: Specify the encryption method for SNMP communication. None and DES are available.

None: No encryption is applied.

DES: Data Encryption Standard (DES) applies a 58-bit key to each 64-bit block of data.

6.3 Coovachilli Settings

Coovachilli is a captive portal management that allows WLAN users to easily and securely access the Internet. Under Router mode, when Coovachilli is enabled, the IEEE 802.11b/g/n Wireless Access Point will force an HTTP client on a network to see a special web page (usually for authentication purposes) before using the Internet normally. The browser is then redirected to a Web page that requires authentication. Captive portals are used at most Wi-Fi hotspots. Therefore, to use Coovachilli, you need to find Coovachilli service providers that have the additional services needed to make Coovachilli work.

The screenshot shows the 'CoovaChilli Settings' page within a web interface titled 'Wireless Broadband Access Point'. The interface has a top navigation bar with 'Status', 'System', 'Wireless', 'Management' (selected), and 'Tools'. A 'Logout' link is in the top right. On the left, a sidebar lists 'Remote Settings' with sub-items: 'CoovaChilli Settings' (selected), 'Firmware Upload', 'Configuration File', 'Password Settings', and 'Certificate Settings'. The main content area is titled 'CoovaChilli Settings' and includes the instruction 'Use this page to set basic CoovaChilli settings.' Below this is a checkbox for 'Coovachilli Enable'. The 'RADIUS Settings' section contains fields for 'Primary RADIUS Server' (radius1.coova.net), 'Secondary RADIUS Server' (radius2.coova.net), 'RADIUS Auth Port' (1812), 'RADIUS Acct Port' (1813), 'RADIUS Shared Secret' (masked with dots), and 'RADIUS NASID' (your-radius-nasid). At the bottom, there is a section for 'RADIUS Administrative-User'.

Figure 6-4. Coovachilli settings.

Radius Settings

Primary Radius Server: Enter the name or IP address of the primary radius server.

Secondary Radius Server: Enter the name or IP address of the primary radius server, if any.

Radius Auth Port: Enter the port number for authentication.

Radius Acct Port: Enter the port number for billing.

Radius Shared Secret: Enter the secret key of the radius server.

Radius NAS ID: Enter the name of the radius server, if any.

Radius Administrative-User

Radius Admin Username: Enter the username of the Radius Administrator.

Radius Admin Password: Enter the password of the Radius Administrator.

Captive Portal

UAM Portal URL: Enter the address of the UAM portal server.

UAM Secret: Enter the secret password between the redirect URL and the Hotspot.

6.4 Upgrade Firmware

Open “Firmware Upload” in “Management” and follow the steps below to upgrade firmware locally or remotely through the Wireless P-T-P Ethernet Extender’s Web interface:



Figure 6-5. Upgrade firmware.

- Click “Browse” to select the firmware file you want to load;
- Click “Upload” to start the upload process;
- Wait a moment, and the system will reboot after a successful upgrade.

CAUTION: Do NOT cut the power off during upgrade; otherwise, the system may crash.

6.5 Backup/ Retrieve Settings

We strongly recommend that you back up configuration information. If tragedy impacts your device, you will have access to restore the important files via backup. This can be done by the local or remote computer.

Open “Configuration File” in “Management” as shown on the next page:



Figure 6-6. Backup/retrieve settings.

Save Setting to File: When you click "Save," a dialog box will pop up. Save it, then the configuration file ap.cfg will be generated and saved to your local computer.

Load Settings from File: By clicking "Browse," a file selection menu will appear; select the file you want to load, like ap.cfg. Click "Upload" to load the file. After automatically rebooting, new settings are applied.

6.6 Restore Factory Default Settings

The Wireless P-T-P Ethernet Extender provides two ways to restore the factory default settings:

Restore factory default settings via Web: From "Configuration File," "Reset" to eliminate all current settings and reboot your device, then default settings are applied.

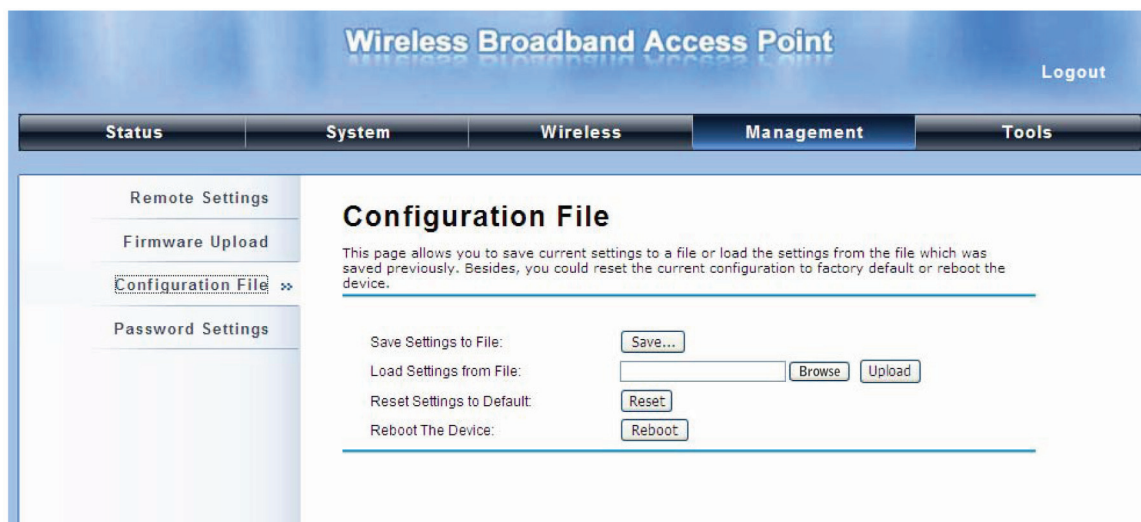


Figure 6-7. Restore settings.

Restore factory default settings via the “Reset” button: If software in the Wireless P-T-P Ethernet Extender unexpectedly crashes and you can no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least five seconds and then release it until the PWR LED blinks.

6.7 Reboot

You can reboot your Wireless P-T-P Ethernet Extender from “Configuration File” in “Management.”

Click “Reboot” and press “Yes” when prompted to start the reboot process. This takes a few minutes.



Figure 6-8. Reboot.

6.8 Password

From “Password Settings” in “Management,” you can change the password to manage your IEEE 802.11b/g/n Wireless CPE.

Enter the new password in both the “New Password” and “Confirm Password” fields; click “Apply” to save the settings.



Figure 6-9. Password.

The password is case-sensitive and it cannot be longer than 19 characters.

6.9 Certificate Settings

In Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The server can trust all certificates issued by a given CA. To import a user certificate, from Import User Certificates, click “Browse” and specify the location where the user certificate is placed. Click “Import.”

The screenshot displays the 'Wireless Broadband Access Point' management web interface. At the top, there is a navigation bar with tabs for 'Status', 'System', 'Wireless', 'Management' (which is active), and 'Tools'. A 'Logout' link is located in the top right corner. On the left side, a sidebar menu lists various settings: 'Remote Settings', 'CoovaChilli Settings', 'Firmware Upload', 'Configuration File', 'Password Settings', and 'Certificate Settings' (which is highlighted with a double arrow). The main content area is titled 'Certificate Settings' and includes the instruction 'Use this page to upload/delete user certificate.' Below this, there are two rows of controls. The first row, 'Delete User Certificate:', features a dropdown menu and a 'Delete' button. The second row, 'Import User Certificates:', features a 'Browse' button and an 'Import' button.

Figure 6-10. Certificate settings.

7. Monitoring Tools

7.1 System Log

System log records events that occur on the Wireless P-T-P Ethernet Extender, including station connection, disconnection, system reboot, etc.

Open "System Log" in "Tools."

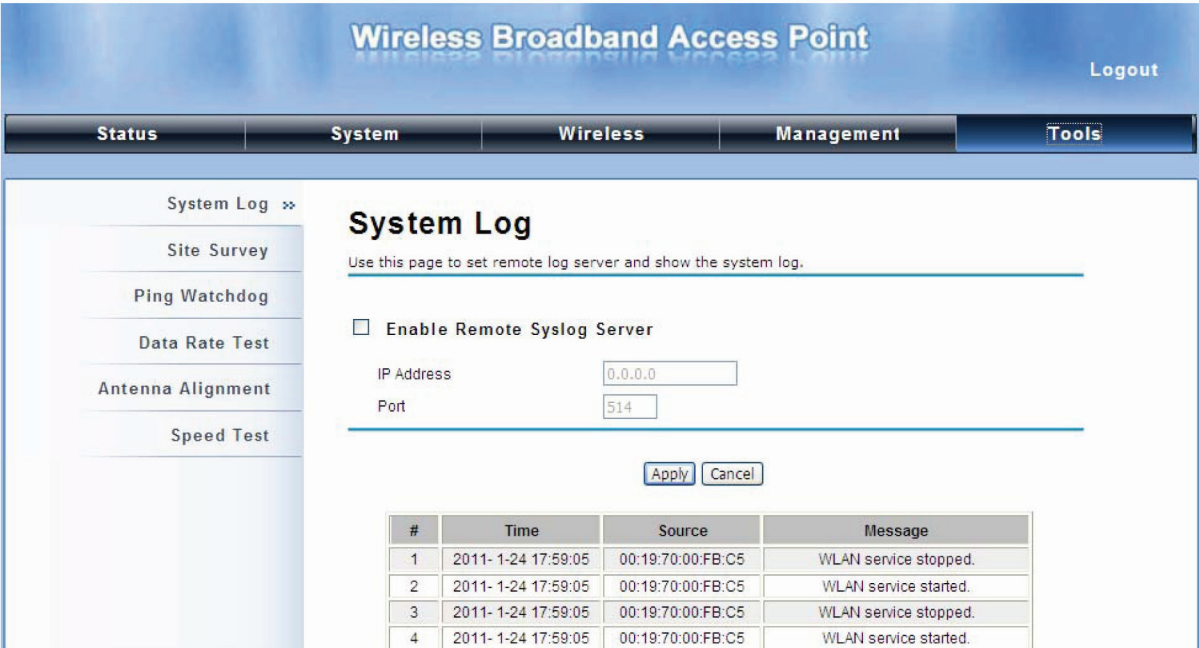


Figure 7-1. System log.

Remote Syslog Server

Enable Remote Syslog: Enable System log to alert remote server.

IP Address: Specify the IP address of the remote server.

Port: Specify the port number of the remote server.

7.2 Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage.

Open "Site Survey" in "Tools" as shown below and select the desired AP to connect.



Figure 7-2. Site survey.

7.3 Ping Watchdog

If the extender unexpectedly disconnects and cuts off your ability the log in to the unit, use the ping watchdog to reboot.



Figure 7-3. Ping watchdog.

Ping Watchdog

Enable Ping Watchdog: To activate ping watchdog, check this checkbox.

IP Address to Ping: Specify the IP address of the remote unit to ping.

Ping Interval: Specify the interval time to ping the remote unit.

Startup Delay: Specify the startup delay time to prevent reboot before the Wireless P-T-P Ethernet Extender is fully initialized.

Failure Count To Reboot: If the ping timeout packets reached the value, the Wireless P-T-P Ethernet Extender will reboot automatically.

7.4 Data Rate Test

The Data Rate Test enables you to test the current RSSI at each data rate between your Wireless P-T-P Ethernet Extenders.

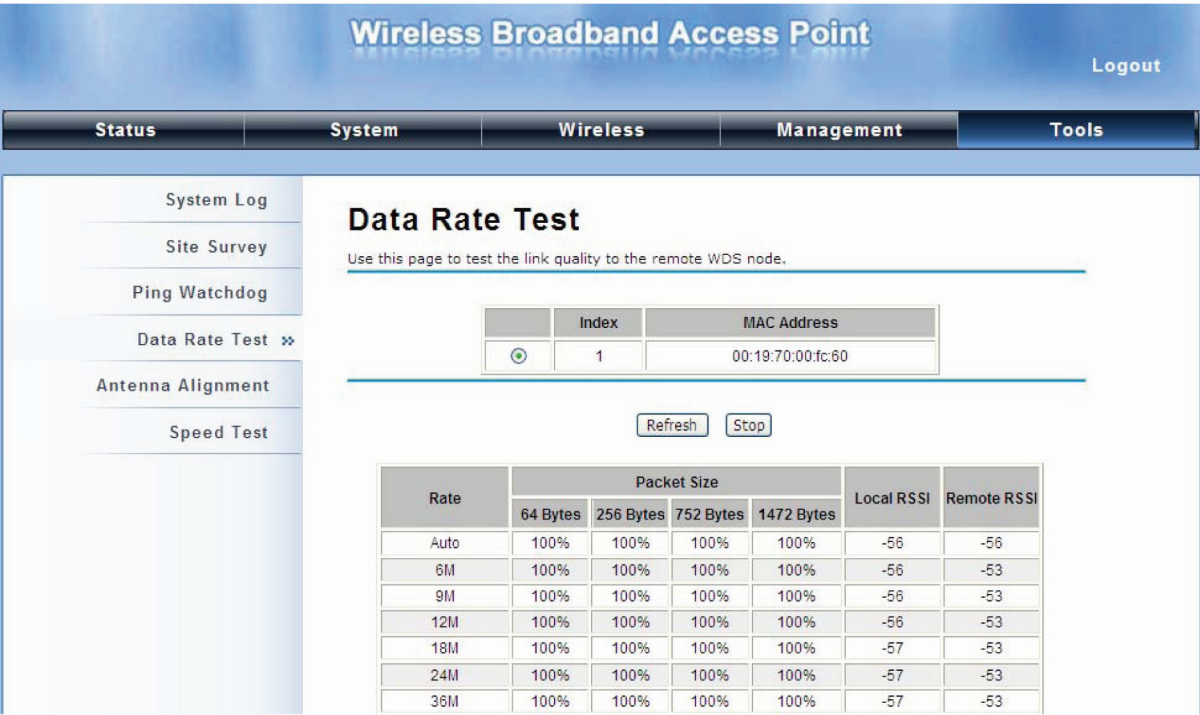


Figure 7-4. Data rate test.

7.5 Antenna Alignment

In Bridge mode, when the bridges are not easily visible from the location where the dish will be installed, the antenna alignment tool can help you evaluate the position of the unit and adjust the angle of the antenna more precisely. Keep in mind that in real circumstances a lot of additional factors should be taken into account when your unit is installed. These factors include various obstacles (buildings, trees), the landscape, the altitude, transponder orientation, polarization, etc.

To use the tool, select the desired remote WDS bridge and click “Start.” The Web page will display the measured signal strength, RSSI, and transmit/receive packets. If the signal quality is not good, adjust the antenna and see if the quality improves.

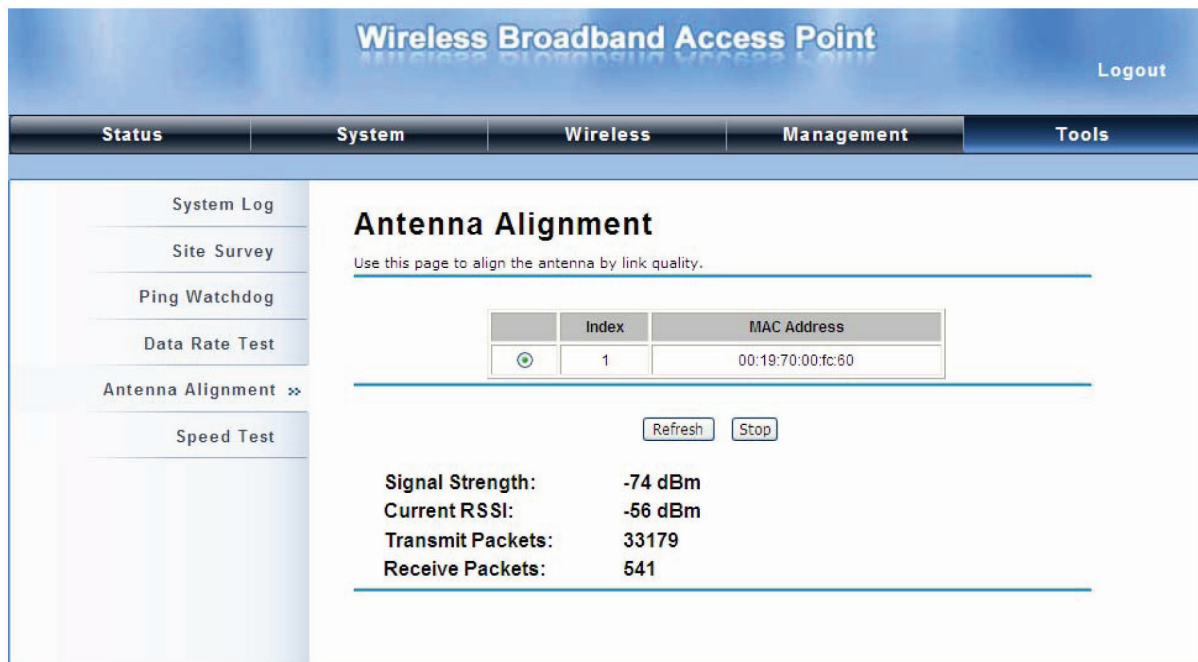


Figure 7-5. Antenna alignment.

7.6 Speed Test

The speed test monitors the current data transmission (TX) and data reception (RX) rate with the remote Wireless P-T-P Ethernet Extender. Enter the IP address of the remote extender, type in the user name/password and click "Test." The result will display in the bottom STATUS. You may test single TX/RX or bi-directional.

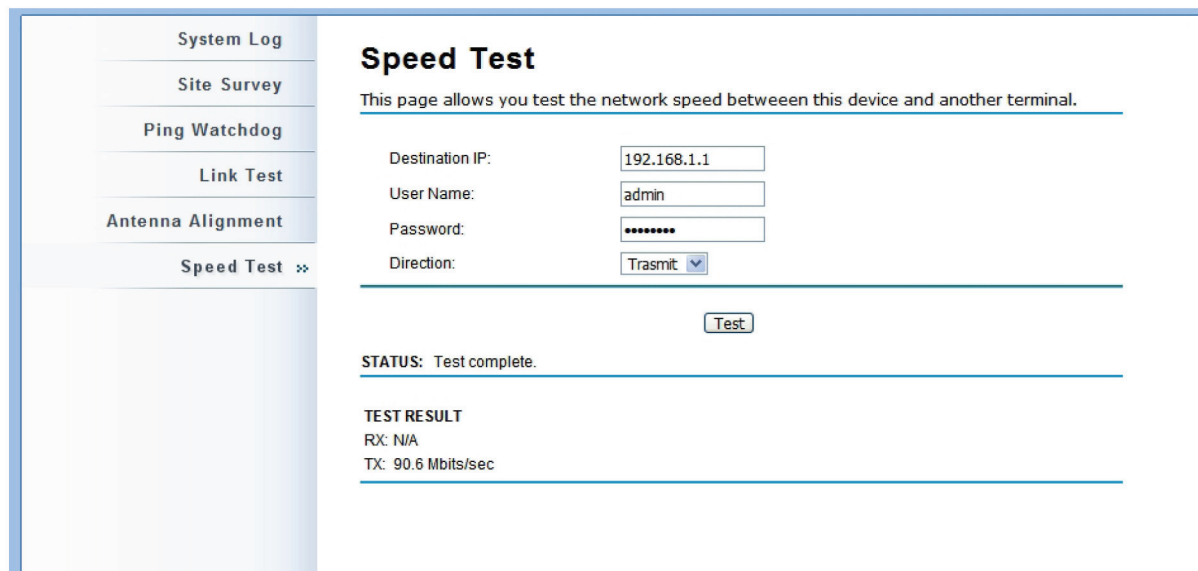


Figure 7-6. Speed test.

8. Status

8.1 View Basic Information

Open “Information” in “Status” to check the basic information of the CPE, which is read-only.

Information includes system information, LAN settings, wireless setting, and interface status. Click “Refresh” at the bottom to get the real-time information.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The main content area is titled 'Information' and contains three sections: 'System Information', 'LAN Settings', and 'Wireless Settings'.

System Information	
Device Name	ap27ebee
MAC Address	00:19:70:27:eb:ea
Country/Region	United States
Firmware Version	3.0.4

LAN Settings	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:19:70:27:eb:ea

Wireless Settings	
Operation Mode	AP
Wireless Mode	802.11b/g/n

Figure 8-1. Basic information.

8.2 View Association List

Open “Connections” in “Status” to check the information for associated wireless devices, such as MAC address, signal strength, connection time, IP address, etc. All are read-only. Click “Refresh” at the bottom to update the current association list.

The screenshot shows the 'Wireless Broadband Access Point' web interface. The top navigation bar includes 'Status', 'System', 'Wireless', 'Management', and 'Tools'. The left sidebar lists 'Information', 'Connections', 'Statistics', 'ARP Table', 'Bridge Table', 'DHCP Clients', and 'Network Activities'. The main content area is titled 'Association List' and contains a table of associated wireless clients.

VAP Index	MAC Address	Signal Strength	Connection Time	Last IP	Action
1	00:19:70:00:fb:c5	-48	2011-1-24 18:09:20	0.0.0.0	---

Refresh

Figure 8-2. Connection.

By clicking on the MAC address of the selected device on the Web, you may see more details including device name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, and current TX/RX packets.

Association Node Details

The details information of association node:

MAC Address	00:13:02:71:35:ba	Negotiated Rate	Last Signal
Device Name		6M	-86 dBm
Connect time	2011-1-24 17:59:33	24M	-87 dBm
Signal Strength	-85 dBm	36M	-85 dBm
Noise Floor	-117 dBm		
ACK Timeout	27		
Link Quality	0%		
Last IP	169.254.17.206		
TX/RX Rate	0/24 MBs		
TX/RX Packets	2/115		
Bytes Transmitted	119		
Bytes Received	10002		

Figure 8-3. Association node details.

8.3 View Network Flow Statistics

Open “Statistics” in “Status” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “Refresh” to view current statistics.

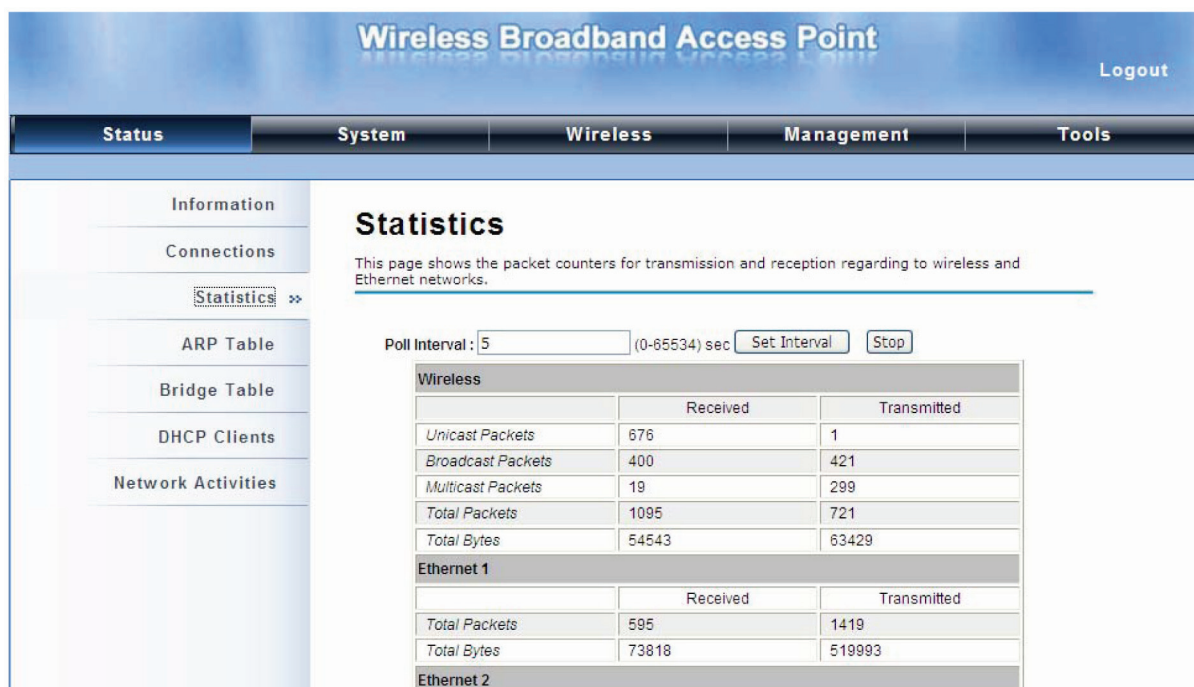


Figure 8-4. Network flow statistics.

Chapter 8: Status

Poll Interval: Specify the refresh time interval in the box beside "Poll Interval" and click "Set Interval" to save the settings. "Stop" discontinues the auto refresh of network flow statistics.

8.4 View ARP Table

Open "ARP Table" in "Status" as shown below. Click "Refresh" to view current table.

The screenshot shows the "Wireless Broadband Access Point" web interface. The top navigation bar includes "Status", "System", "Wireless", "Management", and "Tools". The left sidebar lists "Information", "Connections", "Statistics", "ARP Table" (selected), "Bridge Table", "DHCP Clients", and "Network Activities". The main content area is titled "ARP Table" and contains the text "This table shows ARP table." Below this is a table with three columns: "IP Address", "MAC Address", and "Interface". The table contains one entry: IP Address 192.168.1.111, MAC Address 90:E6:BA:5B:9E:26, and Interface br0. A "Refresh" button is located below the table.

IP Address	MAC Address	Interface
192.168.1.111	90:E6:BA:5B:9E:26	br0

Figure 8-5. ARP table.

8.5 View Bridge Table

Open "Bridge Table" in "Status" as below. Click "Refresh" to view current connected status.

The screenshot shows the "Wireless Broadband Access Point" web interface. The top navigation bar includes "Status", "System", "Wireless", "Management", and "Tools". The left sidebar lists "Information", "Connections", "Statistics", "ARP Table", "Bridge Table" (selected), "DHCP Clients", and "Network Activities". The main content area is titled "Bridge Table" and contains the text "This table shows bridge table." Below this is a table with three columns: "MAC Address", "Interface", and "Ageing Timer(s)". The table contains three entries: MAC Address 00:13:02:71:35:ba, Interface LAN, Ageing Timer(s) 8.78; MAC Address 90:e6:ba:5b:9e:26, Interface LAN, Ageing Timer(s) 0.00; and MAC Address 00:19:70:00:fb:c5, Interface Bridge, Ageing Timer(s) ---. A "Refresh" button is located below the table.

MAC Address	Interface	Ageing Timer(s)
00:13:02:71:35:ba	LAN	8.78
90:e6:ba:5b:9e:26	LAN	0.00
00:19:70:00:fb:c5	Bridge	---

Figure 8-6. Bridge table.

8.6 View Active DHCP Client Table

Open "DHCP Clients" in "Status" as shown below to check the assigned IP address, MAC address, and time expired for each DHCP leased client. Click "Refresh" to view current table.

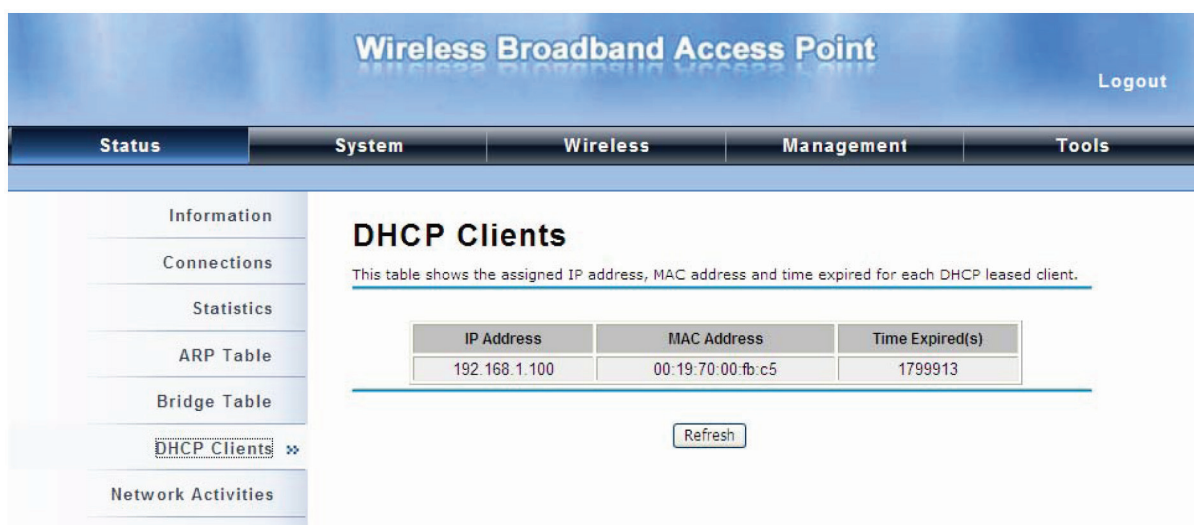


Figure 8-7. DHCP client table.

8.7 View Network Activities

The network activities enables you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Skyport Web. The chart scale and throughput dimension (bps, kbps, Mbps) changes dynamically according to the mean throughput value. You can manually update throughput statistics using the “Refresh” button.

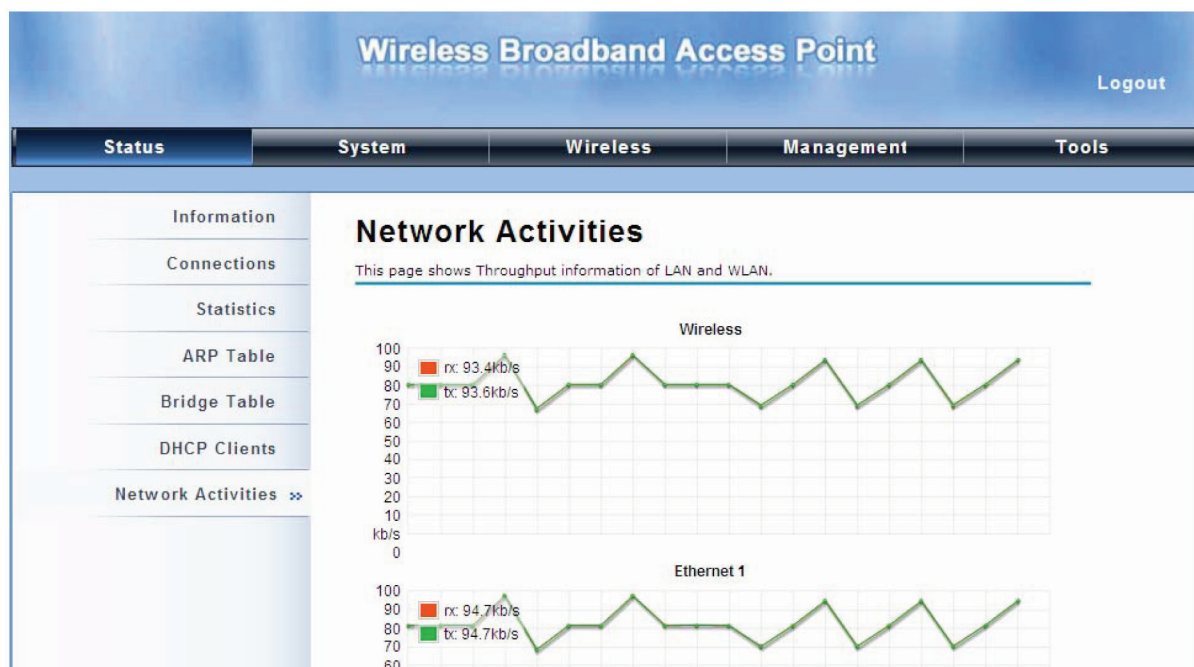


Figure 8-8. Network activities.

9. Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the Wireless P-T-P Ethernet Extender.

9.1 Frequently Asked Questions

Q 1. What is the MAC address of the Wireless P-T-P Ethernet Extender?

MAC Address distinguishes itself by a unique identity among network devices. It appears in two places:

1. Each device has a label posted with the MAC address. Please see below.

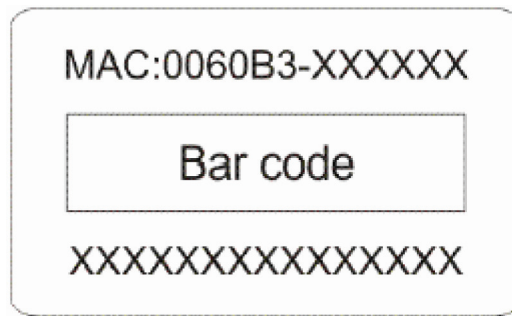


Figure 9-1. MAC address.

2. On the Wireless P-T-P Ethernet Extender Web-based management interface, you can view the MAC Address from "View Basic Information."

Q 2. How do I reset the unit to default settings?

You may restore factory default settings in "Configuration File" from "Management."

Q 3. How do I backup and retrieve my configuration settings?

You backup the file by generating a configuration file or retrieve the settings you have backed up previously in "Configuration File" from "Management."

Q 4. What if I cannot access the Web-based management interface?

Please check the following:

- Make sure the power supply is working; try to power on the unit again.
- Make sure the IP address of PC is correct (in the same network segment as the unit).
- Login to the unit via another browser, such as Firefox.
- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the Wireless P-T-P Ethernet Extender comes with a built-in directional antenna, we recommend that you make the Wireless P-T-P Ethernet Extender face the direction where the AP is for best connection quality.
- In addition, you can start "Site Survey" in "Wireless Basic Settings" to check the signal strength. If it is weak or unstable (the smaller the number is, the weaker the signal strength is), join another available AP for a better connection.

9.2 Contacting Black Box

If you determine that your Wireless P-T-P Ethernet Extender is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

9.3 Shipping and Packaging

If you need to transport or ship your Wireless P-T-P Ethernet Extender:

- Package it carefully. We recommend that you use the original container.
- If you are returning the unit, make sure you include everything you received with it. Before you ship for return or repair, contact Black Box to get a Return Authorization (RA) number.

Appendix A: ASCII

Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ASCII). As defined, the hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of a two-digit hexadecimal.

Table A-1. ASCII.

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
1	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
"	27	?	3F	W	57	o	6F
(28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
-	2A	B	42	Z	5A	r	72
+	2B	C	43	[5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	'	60	x	78
1	31	i	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	(7B
4	34	L	4C	d	64	{	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	-	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Appendix B. SSH Settings

Table B-1. CLI commands.

get	set	del	Keyword				Descriptions
√	√		time				-time setting
√				-now			-current system time
√	√			-zone			-time zone
√	√			-NTPUpdate			-NTP Update
√	√			-servertype			-server type
√	√			-IP			-IP
√	√			-Manual IP			-Manual IP
√	√		system				-system setting
√				-swverson			-system firmware version
√	√			-systemmac			-system MAC address
√	√			-devname			-system name
√	√			-country			-country/region
	√			-ethernet1DataRate			-ether port 1 data rate
√	√			-ethernet2DataRate			-ether port 2 data rate
√	√			-macclone			-mac clone enable
√	√			-clonedmac			-cloned mac address
√	√			-poepower			-secondary RJ45 power
√	√			-stp			-Spaning Tree
√	√			-stpForwardDelay			-STP forward delay
√	√			-gpslatitude			-gps latitude
√	√			-gpslongitude			-gps longitude
√	√		ipset				
√	√			-networkmode			-network mode select (bridge or router)
√	√			-bridge			-bridge mode ip settings
√	√				-iptype		-fixed/dynamical ip (dhcp client)
√	√				-ipaddr		-ip address

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√			-netmask		-subnet mask
√				-gateway		-gateway ip address
√	√			-dns1		-dns1
√	√			-dns2		-dns2
√	√		-router			-router mode ip settings
√	√			-wan		-wan ip settings
√	√				-accesstype	-router mode access type
√	√				-staticipadd	-static ip address
√	√				-staticnetmask	-static subnet mask
√	√				-staticgateway	-static gateway ip address
√	√				-staticdns1	-static dns1
√	√				-staticdns2	-static dns2
√	√				-dhcpcclient hostname	-dhcp client hostname
√					-pppoeconnectstatus	-pppoe connect status
√					-pppoeip	-obtains IP from pppoe server
√	√				-pppoeipaddr	-pppoe static ip address
√	√				-pppoeusername	-pppoe username
√	√				-pppoepassword	-pppoe password
√	√				-pppoeusername	-pppoe server name
√	√				-pppoeconnectmode	-pppoe connect mode
√	√				-pppoeidletime	-pppoe idle time
√	√			-lan		-lan ip settings
√	√				-ipaddr	-lan ip address
√	√				-netmask	-lan subnet mask
√	√				-dhcpserverenable	-dhcp server enable
√	√				-dhcpserveripstart	-dhcp server ip start

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√				-dhcpserveripend	-dhcp server ip end
√	√				-dhcpserverleasetime	-dhcp server leasetime
√	√				-dhcprelayenable	-dhcp relay enable
√	√				-dhcpserverip	-dhcp server ip
√	√		wlan			-wlan setting
√	√			-operationmode		-operation mode
√	√			-ssid		-wireless network name
√	√			-ssidhided		-wireless SSID broadcast
√	√			-radio		-radio switch
√	√			-wirelessmode		-wireless mode
√	√					
√	√			-HTprotect		-HT protect
√	√			-frequency/channel		-wireless frequency/channel (depends on country and wireless mode)
√				-power		-power
√	√			-rate		-rate
√	√			-antenna		-antenna type
√	√			-antennaGain		-antenna gain settings
√	√			-wmm		-wmm settings
√	√			-isolation		-wireless isolate communication between clients
√	√			-maxStaNum		-max sta connection number
√	√			-StaNumLmt		-manually limit the number of stations
√	√			-spaceInMeter		-wireless bwa space in meter setting
√	√			-LinkIntegration		-wireless bwa coverage class setting
√	√			-channelMode		-channel mode
√	√			-channelOffset		-channel offset of 40 MHz
√	√			-extension		-extension

Appendix B. SSH Settings

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√			-A-MPDU		-A-MPDU
√	√			-A-MSDU		-A-MSDU
√	√			-shortGI		-shortGI
√	√			-RIFS		-rifs
√	√			-RTS		-RTS
√	√			-fragment		-fragment
√	√			-beacon		-beacon
√	√			-DTIM		-DTIM
√	√			-preamble		-preamble
√	√			-IGMP		-IGMP
√	√			-stdm		-stdm setting
√	√			-cpeType		-CPE Type
√	√			-authentication		-wireless authentication type
√				-encryption		-wireless data encryption
√	√	√		-key		-wireless wep key setting
√	√				-type	-wireless wep key type
√	√				-default	-wireless wep default key index
√	√	√			-1	-wireless wep key 1
√	√	√			-2	-wireless wep key 2
√	√	√			-3	-wireless wep key 3
√	√	√			-4	-wireless wep key 4
√	√	√		-wpa		-wireless WPA setting
√	√	√			-psk	-wireless pre-shared key (PSK) for WPA-PSK
√	√				-reauthtime	-wireless WPA re-auth period (in seconds)
√	√				-keyupdate	-enable wireless WPA global key update
√	√	√		-eap		-WPA EAP setting

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√	√			-eaptype	-WPA EAP Type
√	√	√			-innereaptype	-WPA inner EAP Type
√	√				-username	-WPA user name
√	√				-loginname	-WPA login name
√	√				-password	-WPA password
√	√				-usercert	-WPA cert file
√	√				-privatekeypassword	-WPA private key password
√	√			-trafficshaping		-traffic shaping
√	√				-enable	-enable Traffic Shaping
√	√				-downlimit	-Incoming Traffic Limit
√	√				-downburst	-Incoming Traffic Burst
√	√				-uplimit	-Outgoing Traffic Limit
√	√				-upburst	-Outgoing Traffic Burst
√				-wdsMac		-WDS Remote Mac
√	√				-local	-local macAddr
√	√				-remote1	-remote macAddr1
√	√				-remote2	-remote macAddr2
√	√				-remote3	-remote macAddr3
√	√				-remote4	-remote macAddr4
√	√			-wdsSeparation		-WDS Separation
√				-association		-list of associated wireless clients
√	√		vapprofile 1 (2,3, etc.)			-VAP setting
√	√			-active		-on/off this vap
√	√			-profileName		-Name of profile
√	√			-ssid		-ssid of this vap
√	√			-ssidhidden		-Broadcast SSID Enable or Disable

Appendix B. SSH Settings

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√			-vlanID		-vlanID of this vap
√	√			-Isolation		-wireless separation
√	√			-wmm		-WMM Support
√	√			-MaxStaNum		-Max Station Number
√	√			-StaNumLmt		-Manually limit the number of stations
√	√			-authentication		-wireless authenticatoin type
√	√			-encyrption		-wireless data encryption
√	√			-default		-wireless wep default key index
√	√			-wpa		-wireless WPA setting
√	√			-association		-list of associated wireless clients
√	√		vlan			-vlan setting
√	√			-active		-enable 802.1Q VLAN
√	√			-manageiD		-Management VLAN ID
√			radius			-radius setting
√	√			-IPAddr		-IP address
√	√			-port		-port
√	√			-shared secret		-Shared Secret
√	√		firewall			-firewall setting
√	√			-srcipfilter		-source ip filter settings
√	√				-enable	-source ip filter enable
√	√				-addrule	-add a source ip filter rule
	√				-delerle	-delete source ip filter rule
√					-rulelist	-show source ip filter rule lists
√	√			-srcpportfilter		-source port filter settings
√	√				-enable	-source port filter enable
√	√				-addrule	-add a source port filter rule

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
	√			-delerule		-delete source port filter rule
√				-rulelist		-show source port filter rule lists
√	√		-destportfilter			-destination port filter settings
√	√			-enable		-destination port filter enable
√	√			-addrule		-add a destination port filter rule
	√			-delerule		-delete destination port filter rule
√				-rulelist		-show destination port filter rule lists
√	√		-portforward			-port forward settings
√	√			-enable		-port forward enable
√	√			-addrule		-add a port forward rule
	√			-delerule		-delete port forward rule
√				-rulelist		-show port forward rule lists
√	√		-dmzenable			-dmz enable
√			-dmzipaddr			-dmz ip address
√	√		remote			-remote management setting
√	√		-privacy			-radius IP address
√	√		-telnet			-enable telnet
√	√		-snmp			-enable snmp
√	√		-ftp			-enable ftp
√	√		-ssh			-enable ssh
√	√		-forcehttps			-force https
√	√		-wise			-enable wise tools
√	√		snmp			-SNMP setting
√	√		-version			-Protocol Version
√	√		-port			-Server Port
√	√		-getCommunity			-SNMP Read Community

Appendix B. SSH Settings

Table B-1 (Continued). CLI commands.

get	set	del	Keyword			Descriptions
√	√			-setCommunity		-SNMP Write Community
√				-trapdestination		-Trap Destination
√	√			-trapcommunity		-Trap Community
√	√			-v3Admin		-v3Admin
√	√				-on	-Enable SNMPv3Admin
√	√				-name	-name
	√				-password	-password
√	√				-accessType	-access type
√	√				-authetica	-Authentication Protocol
√	√				-Privacy	-privacy protocol
√	√			-v3User		-v3User
√	√				-on	-Enable SNMPv3User
√	√				-name	-name
√					-password	-password
√	√				-accessType	-access type
√	√				-authentication	-Authentication Protocol
√	√				-Privacy	-privacy protocol
√	√		coovachilli			-CoovaChilli setting
√	√			-coovaChilliEnable		-Coovachilli Enable
√	√			-primaryRadiusServer		-Primary RADIUS Server
√	√			-secondaryRadiusServer		-Secondary RADIUS Server
√	√			-radiusAuthPort		-RADIUS Authentication Port
√	√			-radiusAcctPort		-RADIUS Accounting Port
√	√			-radiusSharedSecret		-RADIUS Shared Secret
√	√			-radiusNasid		-RADIUS Nasid
√	√			-radiusAdminUsername		-RADIUS Admin Username

Table B-1 (Continued). CLI commands.

get	set	del	Keyword				Descriptions
√	√			-radiusAdminPassword			-RADIUS Admin Password
√				-uamPortalUrl			-UAM Portal URL
√	√			-uamSecret			-UAM Secret
√	√		syslog				-syslog
√	√			-client			-enable syslog client
√	√			-ipaddr			-syslog server IP address
√	√			-port			-syslog server port number
√	√			-clear			-syslog clear
√	√		pingwdg				-ping watchdog
√	√			-enable			-enable
√	√			-interval			-interval
√	√			-startdelay			-startup delay
√	√			-failcount			-failure count
√				-ip			-ip address
√	√	√	acl				-access control
√	√			-mode			-enable wireless access control (ACL)
		√		-delete			-delete a local ACL
√		√		-list			-delete or display all local ACL addresses
	√			-MacAddr			-add mac address to Current Access Control List
√			statistics				-statistics
√				-Wireless			-Wireless LAN
√				-Ethernet			-Ethernet LAN
√		√	log list				-syslog list
	√		password				-system password
	√		reset				-restore factory
	√		reboot				-reboot system
	√		exit				-logout from CLI

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.



Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.



About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech Support available in 30 seconds or less.

© Copyright 2012. Black Box Corporation. All rights reserved.